GURUFIN

GLOBAL ON-CHAIN FX/DeFi HUB FOR WEB3 ECONOMY

A public DPoS Layer-1 for stablecoins, tokenized assets, and cross-border payments.

Government, Central Bank, FMIs Institutional Edition
GURUFIN Technical Papers Series V. 2-2025
September 2025

CONTENTS

Foreword

The evolution of money and payments has reached a pivotal juncture. While global finance has been transformed by digitalisation, both legacy infrastructures and blockchain-based systems continue to face structural inefficiencies, fragmented liquidity, volatile fees, and unsafe cross-chain mechanisms. Addressing these challenges requires solutions that combine technological innovation with the institutional safeguards of trust, compliance, and resilience.

Gurufin has been conceived as a neutral, public Layer-1 settlement hub that bridges stablecoins, tokenised assets, and cross-border payments. Built on an IBC-first architecture with EVM compatibility, Gurufin integrates deterministic payment-versus-payment atomicity, fiat-predictable fees through Guru-PEG, and market-grade observability. It is designed not merely as another blockchain, but as an institutional-grade financial market infrastructure for the Web3 economy, aligning innovation with regulatory legibility and global interoperability.

This paper presents the vision, architecture, and governance model of Gurufin. It is intended for policymakers, financial institutions, developers, and market participants who share the goal of advancing a safer, more efficient, and inclusive foundation for global value exchange.

GLOBAL ON-CHAIN FX/DeFi HUB FOR WEB3 ECONOMY*:*

A public DPoS Layer-1 for stablecoins, tokenized assets, and cross-border payments.

Gurufin, Blockchain Research Labs
September 2025.

Abstract

This paper presents Gurufin, a public, permissionless Delegated Proof-of-Stake (DPoS) Layer-1 protocol designed as a neutral foreign exchange (FX) and settlement hub for fiat-backed stablecoins and tokenized assets. The scope of Gurufin is to provide institutional-grade interoperability and predictable cross-border settlement by embedding FMI-style safeguards into a blockchain-native environment.

Methodologically, Gurufin integrates Inter-Blockchain Communication (IBC) as its default interoperability protocol, complemented by an Ethereum Virtual Machine (EVM) gateway. Safety and predictability are enforced through payment-versus-payment (PvP) atomic settlement, fiat-indexed fee equilibrium (Guru-PEG), and a hybrid execution fabric combining automated market makers (AMMs) with request-for-quote (RFQ) venues. Data integrity is maintained via a decentralized oracle network and supervisory-grade observability, while optional zk-proof-assisted privacy modes and compliance hooks align the system with FATF and jurisdictional requirements.

The results demonstrate that Gurufin can minimize bridge risk, compress spreads, and deliver fiat-like fee stability, while providing regulators and supervisors with transparent, auditable telemetry. This paper contributes a reference architecture, governance framework, and compliance model for building a globally interoperable and regulator-ready cross-border settlement infrastructure.

Keywords: *Cross-border payments, stablecoins, tokenized assets, Delegated Proof-of-Stake (DpoS), Inter-Blockchain Communication (IBC), Ethereum Virtual Machine (EVM), payment-versus-payment (PvP), Automated Market Makers (AMM), Request-for-Quote (RFQ), canonical asset registry, oracles, DexAggregator, zk-proof privacy, Financial Market Infrastructure (FMI), cross-chain settlement, regulatory compliance, Web3 economy.*

1. Hypothesis

The global financial system continues to face persistent inefficiencies rooted in both legacy infrastructures and current-generation blockchain protocols. Traditional cross-border settlement depends on RTGS systems, SWIFT messaging frameworks, and pre-funded correspondent banking networks, each of which introduces delays, elevated costs, and exclusionary access structures. These frictions are especially acute for retail remittances and small enterprise flows, where intermediated liquidity and manual reconciliation inflate spreads and settlement times.

Parallel to this, blockchain networks have yet to achieve FMI-grade reliability. Auction-based gas markets expose participants to volatile and unpredictable fees, undermining budget certainty for both retail and institutional actors. Moreover, cross-chain interoperability is often attempted through wrapped-asset bridges, which introduce custodial dependencies, synthetic inflation risks, and repeated episodes of de-pegging, thereby eroding systemic trust. Liquidity is further fragmented across multiple venues and asset representations, creating inefficiencies in price discovery and widening bid–ask spreads.

Gurufin hypothesizes that these dual limitations can be resolved by establishing a neutral, public, compliance-ready FX and settlement hub ("Neutral FX/DeFi hub"), designed to embed FMI-grade safeguards into the Web3 environment. Specifically:

Volatile fees → predictable pricing: The Guru-PEG mechanism normalizes gas costs in fiat terms (CPI-indexed), ensuring retail-grade predictability while preserving validator incentives.

Principal and bridge risk → PvP atomicity: An IBC-first design enforces escrow-based, proof-verified payment-versus-payment (PvP) atomic settlement, thereby eliminating unilateral exposure and aligning with BIS delivery-versus-payment principles.

Liquidity fragmentation → unified execution fabric: A hybrid model integrates AMM liquidity for small-scale flows and RFQ venues for institutional tickets, supplemented by a governance-controlled canonical

asset registry to prevent split liquidity and maintain efficient spreads.

Opacity in oversight → transparent observability: A market-grade telemetry stack publishes real-time data on slippage, spreads, Oracle health, and governance events in machine-readable form, enabling FMI-style supervisory visibility.

Privacy vs compliance trade-off → audit-compatible confidentiality: Zk-assisted privacy modes and wallet-tier compliance checks preserve user confidentiality while remaining verifiable under FATF Travel Rule frameworks.

By combining deterministic finality, fiat-predictable fees, safe cross-chain interoperability, and audit-compatible privacy, Gurufin advances the hypothesis that a neutral, public Layer-1 settlement hub can harmonize Web3 innovation with the standards of trust, resilience, and regulatory legibility demanded by global financial markets.

2. High-Level Architecture

The foundational Gurufin layer, or mainnet, is built upon the Cosmos SDK and leverages Inter-Blockchain Communication (IBC) as its primary interoperability protocol, as it is represented in Figure 1, ensuring secure and scalable asset transfers across heterogeneous domains. This execution environment, referred to as the Neutral FX/DeFi hub, integrates an EVM gateway to extend compatibility with Ethereum-based assets, liquidity, and developer tooling.

Together, these components establish Gurufin's role as a settlement hub where stablecoins and cross-border payment flows can interoperate with minimal friction. By combining the modularity of Cosmos, the safety of IBC, and the extensibility of EVM compatibility, the Gurufin Mainnet provides the foundation for all higher-level functions, including governance, compliance, and privacy layers.

The architecture of Gurufin is founded on a *Delegated Proof-of-Stake* (DPoS)[1] governance chain, employing a consensus engine akin to *Tendermint*[2] to achieve deterministic finality and granular protocol control [1].

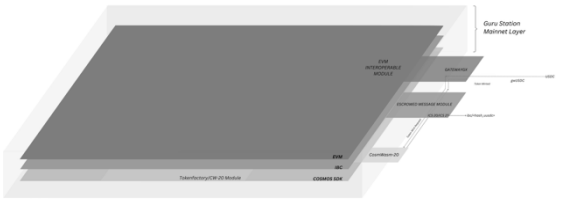


Figure 1 Neutral FX/DeFi hub - L1 Mainnet Layer

Additionally, an execution fabric (Neutral FX/DeFi hub) specialised for FX and cross-chain settlement interoperability is provided via the *Inter-Blockchain Communication* [3] (IBC) protocol, enabling trust-minimised, message-based, atomic escrow[4] and cross-chain settlement across heterogeneous systems [1], [2], [3].

An EVM gateway[5] enables seamless integration with Ethereum-compatible liquidity and developer tooling, supported by atomic cross-chain innovative contract execution mechanisms, such as *IntegrateX*[6], which ensure efficiency and transaction integrity across EVM domains [4].

A privacy layer combines zero-knowledge proof (*zk-proof*[7]) capabilities with optional Trusted Execution Environments[8] (TEEs), inspired by systems such as *Ekiden*, to enable confidential yet high-performance execution where required [5], [6], [7].

Finally, a market-grade observability stack tracks performance and compliance metrics across the entire stack.

[1] Delegated Proof of Stake (DPoS) is a consensus algorithm where token holders elect a limited set of validators to produce blocks, enabling deterministic finality, higher throughput, and governance flexibility compared to classical Proof of Stake.

[2] Tendermint is a Byzantine Fault Tolerant (BFT) consensus engine that provides deterministic finality and high throughput by combining a blockchain replication protocol with a Proof-of-Stake validator set, widely used as the consensus core for Cosmos and other networks.

[3] Inter-Blockchain Communication (IBC) is a protocol that enables secure and trust-minimized interoperability between heterogeneous blockchains by using light-client proofs, authenticated channels, and message passing to support atomic cross-chain transactions and asset transfers.

[4] Atomic escrow is a cross-chain settlement mechanism where assets on each participating chain are placed into conditional escrow contracts, and are only released if all legs of the transaction satisfy predefined proofs within timeout windows, ensuring payment-versus-payment (PvP) atomicity and eliminating single-leg settlement risk.

[5] An EVM gateway is an interoperability module that connects non-Ethereum blockchains to Ethereum-compatible networks, enabling cross-chain asset transfers and seamless integration with Ethereum's smart contracts, liquidity, and developer tooling.

[6] IntegrateX is a cross-chain framework that enables atomic, high-efficiency smart contract execution across heterogeneous blockchains, ensuring both transaction integrity and low latency in interoperability scenarios.

[7] A zero-knowledge proof (zk-proof) is a cryptographic method that enables one party to prove knowledge of specific information to another party without revealing the underlying data itself, thereby ensuring privacy while maintaining verifiability.

[8] A Trusted Execution Environment (TEE) is a secure area of a processor that isolates code and data from the main operating system, providing confidentiality, integrity, and attestable execution even in the presence of potentially compromised system software.

Design goals:

i. Predictable, low-latency finality.
ii. PvP atomic settlement across chains.
iii. Stable, fiat-like fees.
iv. Safety-first interop via IBC
v. Rich telemetry for users, venues, and supervisors.

2.1 Governance Chain (DPoS core)

The governance chain, as shown in Figure 1, runs a *Tendermint-class BFT* engine with delegated proof-of-stake, providing block times of ~1–3 seconds and five-figure TPS on commodity infrastructure.

It uses the Guru native token (GXN).

Enforces *DPos slashing/jailed states*[9] on *Tendermint* for equivocation/downtime (Figure 2), and exposes on-chain governance for parameters, listings, and upgrades.

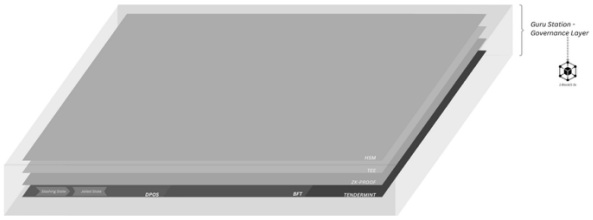


Figure 2 Neutral FX/DeFi hub - Governance Layer

External entities are encouraged to run validators; minimum specs and staking thresholds are published.

The chain is the control plane for:

- Parameter changes (fee bands, Oracle sets).
- Listing/venue governance.
- Upgrade coordination with rollback hooks.
- Security policy (key rotation, emergency halts under community vote).

2.2 Neutral FX/DeFi hub **(FX execution layer)**

Gurufin's primary purpose is to serve as a neutral FX settlement hub that aggregates liquidity from both Automated Market Makers[10] (AMMs) and Request-for-Quote[11] (RFQ) providers, enabling efficient price discovery across stablecoin corridors.

On this foundation, Gurufin ensures that same-chain swaps are settled atomically, while cross-chain swaps achieve *payment-versus-payment*[12] (PvP) atomicity through escrowed holds, guaranteeing that neither leg of a transaction completes unless both are successfully executed[9], [10], [11].

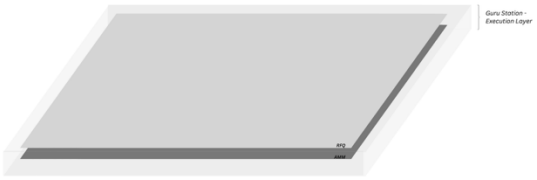


Figure 3 Neutral FX/DeFi hub - Execution Layer

This design eliminates *principal risk*[13] and positions *Gurufin* as a trusted layer infrastructure, as is presented in Figure 4, for digital asset foreign exchange[12].

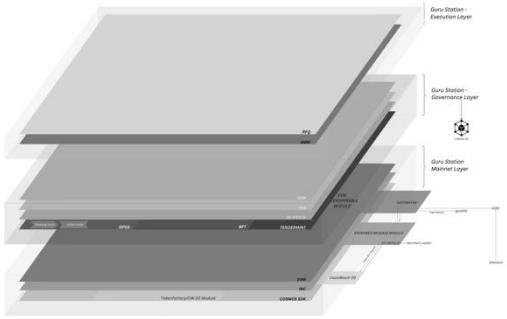


Figure 4 Neutral FX/DeFi hub – Multi-Layer

Pools[14] in Gurufin are optimised for stablecoin ↔ stablecoin pairs (e.g., USGX/KRGX/USDC), where constant-product (k) or stable-swap AMMs can provide deep liquidity and efficient execution for retail and corridor-sized trades (6).

AMMs are particularly effective here because they enable continuous liquidity and predictable pricing,

[9] Slashing and jailed states are security mechanisms in Proof-of-Stake blockchains where validators that misbehave, such as double-signing or prolonged downtime, are financially penalized (slashing) and temporarily or permanently excluded from block production (jailed), thereby preserving network integrity.

[10] An Automated Market Maker (AMM) is a decentralized exchange mechanism where users trade directly against algorithmic liquidity pools, with token prices determined by mathematical invariants (e.g., the constant product formula x·y=kx \cdot y = kx·y=k) rather than order books.

[11] A Request-for-Quote (RFQ) is a trade execution model where a user solicits binding price quotes from designated liquidity providers, enabling large or customized orders to be filled with reduced slippage compared to automated market maker pools.

[12] Payment-versus-Payment (PvP) is a settlement mechanism that ensures the final transfer of one currency occurs *if and only if* the final transfer of the counter-currency also occurs, thereby eliminating principal risk in foreign exchange transactions.

[13] Principal risk, also known as Herstatt risk, is the risk that one party to a foreign exchange transaction delivers the currency it sold but does not receive the currency it bought, due to counterparty default or settlement failure.

[14] A liquidity pool is a smart contract that holds reserves of two or more tokens, allowing users to trade directly against the pooled assets under predefined rules (e.g., AMM invariants), while liquidity providers deposit tokens into the pool and earn fees in return.

even for small transactions, while minimising slippage[15] when trade sizes are modest relative to pool depth, as the simulation explains in Table 1 and Figure 5.

However, for *large-ticket*[16] institutional flows, AMMs alone are inefficient since *slippage* grows significantly with trade size due to the *reserve ratio* shift [9], [13].

Trade Size (% of pool)	Input (USDC)	Output (DAI)	Effective Price (USDC/DAI)	Slippage (%)
0.01	100.0	99.99	1.0001	0.01
0.1	1000.0	999.001	1.001	0.1
0.5	5000.0	4975.1244	1.005	0.5
1.0	10000.0	9900.9901	1.01	1.0
2.0	20000.0	19607.8431	1.02	2.0
5.0	50000.0	47619.0476	1.05	5.0
10.0	100000.0	90909.0909	1.1	10.0
20.0	200000.0	166666.6667	1.2	20.0
30.0	300000.0	230769.2308	1.3	30.0
40.0	400000.0	285714.2857	1.4	40.0
50.0	500000.0	333333.3333	1.5	50.0

Table 1 AMM Slippage vs Trade Size

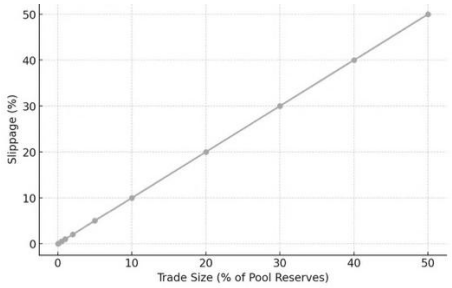


Figure 5 Slippage AMM Vs Trade Size Relative To Pool Size

To address this, *Gurufin* integrates *Request-for-Quote* (RFQ) paths, allowing professional liquidity providers to quote competitive, *low-basis-point*[17] spreads for high-value trades (See Gurufin Execution Layer on Figure 4).

This hybrid approach ensures that retail users benefit from always-on AMM liquidity (Figure 6), while institutions access tailored RFQ pricing for block trades[14].

The slippage curve (Figure 5) highlights why Gurufin Station adopts a hybrid liquidity model, as shown in Figure 4. In the retail zone (small trades), AMM pools deliver near-frictionless execution with negligible slippage, ensuring efficient remittance corridors.

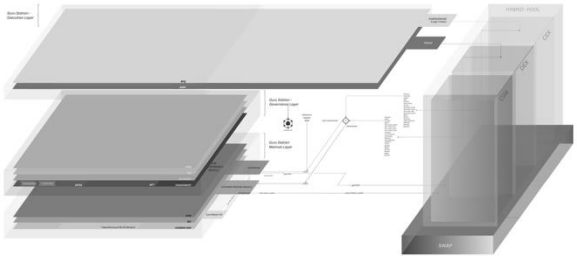


Figure 6 Neutral FX/DeFi hub – FX Hybrid Pool

In the corridor zone (Figure 8), AMMs remain viable, but Gurufin selectively route through RFQ providers when pool depth is insufficient to maintain competitive spreads.

In the institutional zone (large tickets), Gurufin relies on RFQ execution to eliminate excessive slippage (Table 1), allowing professional participants to access low basis point pricing comparable to interbank FX.

Finally, *arbitrage* [18] automation across venues continuously compresses spreads, aligning AMM pool prices with RFQ quotes and external markets, thereby preserving *Gurufin's* role as a neutral FX settlement hub [15].

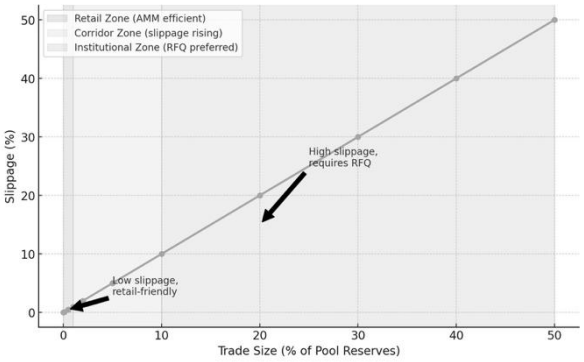


Figure 6 Slippage in AMM Vs Trade Size Relative to Pool Size

The venue model in *Gurufin Station* defines how different trading environments are structured and governed to serve both retail and institutional users.

[15] Slippage is the difference between the expected price of a trade and the actual execution price, commonly caused by liquidity constraints, price impact of large orders, or latency in order processing.

[16] In financial markets, a large ticket refers to a single trade order with high notional value, typically executed by institutional participants, where specialized execution methods (e.g., RFQ) are required to minimize market impact and slippage.

[17] In financial markets, a basis point (bp) is equal to one hundredth of a percent (0.01%), and low basis point pricing refers to transaction costs or spreads quoted at very small increments, typically 1–10 bps (0.01–0.10%), as is common in institutional foreign exchange and money markets.

[18] Arbitrage is the practice of simultaneously buying and selling the same or equivalent assets in different markets to profit from price discrepancies, thereby enforcing price alignment and market efficiency.

On the retail side, *Gurufin Station* supports Decentralised Exchange (DEX) [19] pools with concentrated liquidity and yield programs, ensuring continuous access to stablecoin corridors.

For institutional workflows, *Gurufin Station* can interoperate with Centralised Exchanges (CEX) and RFQ operators, enabling *quote-driven* execution for large-ticket trades with minimal slippage (Table 2).

Feature	CEX (Centralized Exchange)	DEX (Decentralized Exchange)
Asset Custody (Pools)	Custodial wallets controlled by the exchange operator.	On-chain smart contract liquidity pools provided by LPs.
Trading Zone	Centralized order book (matching engine operated by the CEX).	On-chain swap zone (AMM pools or decentralized order books).
Settlement	Internal, off-chain: balances updated in the CEX's database.	On-chain, atomic: swaps execute directly on the blockchain.
Trust Model	Requires trust in the exchange's solvency and operations.	Trust-minimized: governed by smart contracts and consensus rules.
Import into Gurufin	Withdrawals → imported via Eureka Gateway → *gwAssets*.	Cosmos DEXs via IBC → *ibcAssets*; non-Cosmos DEXs via Eureka → *gwAssets*.

Table 2 CEX vs DEX: Pools, Trading Zones, and Settlement

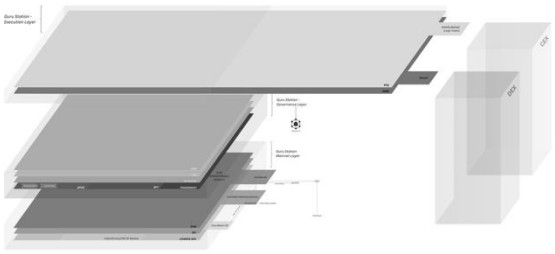


Figure 7 Neutral FX/DeFi hub - Pooling

Across all venues, pool fees, maker–taker schedules, and inventory bands are transparently governed and published on-chain, ensuring predictable economics and compliance alignment.

This *multi-venue* framework allows *Gurufin* to function as a neutral FX settlement hub, harmonising liquidity across AMM pools, RFQ desks, and external markets.

2.3 Interoperability, IBC-first + EVM gateway

IBC as default: Gurufin prioritises IBC as the default mechanism for inter-chain settlement because it provides a trust-minimised, consensus-verified channel for asset transfers. Unlike custodial bridges that rely on wrapped tokens and third-party validators, IBC uses escrowed message passing (ICS-20/27) to enforce Payment-versus-Payment (PvP) across ledgers, ensuring that assets move only when both sides are securely validated.

This approach not only reduces systemic *bridge risk*[20] but also aligns with Gurufin's role as a neutral, regulator-legible FX settlement hub. This aligns with "distributed exchange" principles and reduces bridge risk [16].

Principles:

- *Trust-Minimization*
- *Escrow-Based Transfers (No Synthetic Inflation)*
- *Deterministic Settlement*
- *Transparency & Auditability*
- *Neutral Interoperability*

GatewayGX: The GatewayGX [21] provides Gurufin with interoperability to Ethereum- and Solana-class networks that do not natively support IBC (Figure 1).

The module monitors external chain events and translates them into internal IBC calls, thereby preserving the trust-minimised settlement model. In these cases, wrapped[22] assets are introduced under a narrowly defined scope and governed by a dual-control framework:

(i) Oracles [23], which supply verified external price and status data to validate transfer conditions, and

(ii) Timeout safeguards[24], which ensure that any incomplete or unconfirmed transaction is automatically reversed to prevent exposure to bridge risk [5], [17], [18].

Contracts are deployed symmetrically on both host and guest chains, enabling transparent lifecycle management and allowing for the rapid activation or deactivation of specific routes when circumstances require.

[19] A Decentralized Exchange (DEX) is a blockchain-based trading platform that enables users to swap digital assets directly via smart contracts without relying on centralized intermediaries, typically using automated market makers (AMMs) or order-book protocols.

[20] Bridge risk refers to the security and systemic risks associated with blockchain bridges, including vulnerabilities to smart contract exploits, validator collusion, and liquidity fragmentation caused by unbounded wrapped token issuance.

[21] The GatewayGX is Gurufin's interoperability module for non-IBC blockchains such as Ethereum and Solana, which tracks external events and invokes internal IBC calls, while issuing narrowly scoped wrapped assets under Oracle- and timeout-controlled logic to reduce bridge risk.

[22] A wrapper is a tokenized representation of an external blockchain asset created on a host chain through a bridge or gateway; the wrapper maintains a claim on the original asset but introduces risks such as liquidity fragmentation and depegging if not strictly governed.

[23] An Oracle is a service that supplies blockchains and smart contracts with verified external data, such as asset prices, interest rates, or compliance information, thereby bridging on-chain execution with off-chain real-world events.

[24] Timeout safeguards are risk-control mechanisms in cross-chain protocols that automatically cancel or reverse transactions if required confirmations are not received within a predefined time window, thereby preventing indefinite asset lock-up or incomplete settlement.

2.4 Liquidity layer: pools, pairs, wrappers

Pools and Denominations (*denoms*): Liquidity pools on Gurufin are instantiated with *GXN-denominated* base pairs, ensuring that pricing and settlement remain anchored to the native governance token.

All assets admitted into these pools follow a standardized denomination format that reflects their provenance and transfer route.

For IBC assets, the denomination is expressed on-chain in accordance with the ICS-20 standard [19] [25]:

ibc/<hash>

The <hash> component represents the unique identifier generated from the IBC transfer path, which always terminates in the underlying micro-denomination.

ibc/<hash_uusgx>

Denotes USGX imported from a GX Stablecoin Chains via IBC.

while,

ibc/<hash_uusdc>

Denotes USDC imported from the Noble chain.

This scheme provides a transparent and verifiable method for asset representation, enabling consistent treatment of tokens across pools and preventing liquidity fragmentation.

Gateway-wrapped assets (non-IBC): For networks that do not natively support IBC, such as Ethereum or Solana, *Gurufin* employs the GatewayGX to admit external assets under controlled conditions (Figure 8). These tokens are minted within Gurufin using the *tokenfactory*/CW-20 module shown in Figure 1 and are assigned a dedicated namespace.

To distinguish them from canonical IBC imports, they are referenced with a *gw* alias* in documentation and user interfaces:

gwUSDC

or

gwUSDT.

This convention ensures that market participants can easily identify the asset's origin and risk profile.

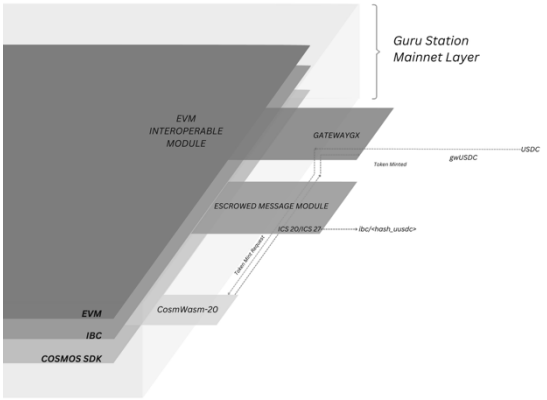


Figure 8 Neutral FX/DeFi hub - Wrapping

Notation (IBC Denominations):

For readability, IBC assets are described in the form:

ibc/<hash_baseDenom>

e.g., ibc/<hash_uusgx>

Although on-chain, they are stored simply as:

ibc/<hash>

The underlying base denomination:

uusgx, uusdc

It is always preserved in the *"denom"* trace, which provides verifiable provenance of the transfer path.

2.4.1 Stablecoin pool topology

Gurufin's liquidity structure is organized around Cosmos-native settlement pools (CSM pools), which establish each admitted stablecoin in relation to GXN as the base anchor. This design ensures consistent accounting, unified governance control, and transparent denomination tracking across all settlement routes.

Examples of these foundational pools include:

ibc/<hash_uusgx> ↔ GXN

ibc/<hash_uusdc> ↔ GXN

and,

gwUSDC ↔ GXN[26]

[25] ICS-20 is the Inter-Blockchain Communication (IBC) token transfer standard that specifies how fungible tokens are escrowed, transmitted, and redeemed across heterogeneous blockchains using channel identifiers and denom traces to preserve provenance.

[26] Subject to governance approval of the route.

Canonical IBC assets (e.g., USGX or USDC from Noble) are represented as:

ibc/<hash_baseDenom>

Executed under the ICS-20 standard, where the <hash> component reflects the IBC transfer path and the base denomination is preserved in the *denom* trace for full provenance (Figure 1):

uusgx
uusdc

Gateway-wrapped assets from non-IBC networks (e.g., Ethereum or Solana) are minted via GatewayGX module using the *tokenfactory/CW-20 framework* and clearly marked with a *gw* alias:

gwUSDC

As shown in the Neutral FX/DeFi hub *Mainnet Layer* on Figure 9, ensuring that participants can distinguish between canonical and non-canonical representations [20], [21], [22].

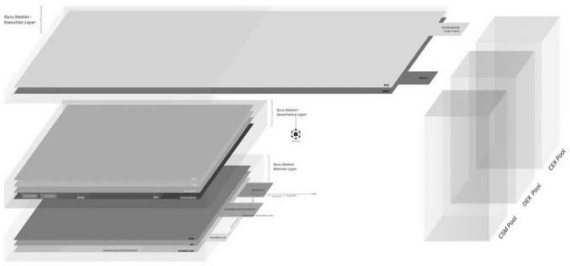


Figure 9 Neutral FX/DeFi hub - CSM Pool

Once governance verifies sufficient *liquidity depth* and asset provenance reliability, Gurufin activates direct stablecoin-to-stablecoin pools:

ibc/<hash_uusgx> ↔ ibc/<hash_ukrgx>

These direct pools minimise reliance on GXN as an intermediary settlement leg, thereby reducing FX exposure and mitigating slippage for cross-currency transactions.

2.4.2 LP tokens and incentives

Liquidity Providers (LPs) who contribute assets to Gurufin pools receive LP tokens:

GXT-<poolID>

Those represent their proportional claim on the pool's reserves. These tokens can be redeemed for the underlying assets plus accrued fees, aligning provider incentives with pool performance [9].

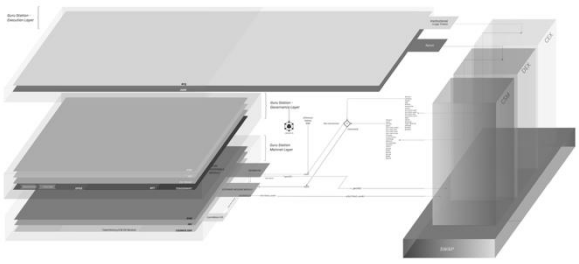


Figure 10 Neutral FX/DeFi hub - Pool Swap

In addition to *fee-based* earnings, *Gurufin* employs pool-specific incentive programs, including governance-approved bonding mechanisms and yield farming rewards, to encourage long-term liquidity provision and mitigate the volatility of shallow depth [23].

To improve capital efficiency, Gurufin integrates concentrated-liquidity AMM models (like Uniswap v3), which allow LPs to allocate capital within defined price ranges rather than across the entire curve.

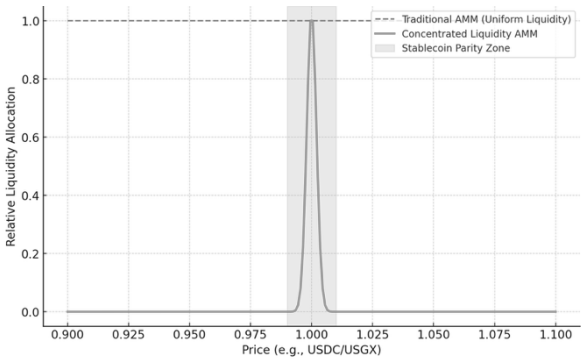


Figure 11 Liquidity Distribution: Uniform Vs Concentrated (Stablecoin Corridors)

This design significantly reduces *idle liquidity*[27] and enhances execution quality for traders, particularly in stablecoin-to-stablecoin corridors where prices cluster around parity [24].

Governance-controlled bonding and staking programs further reward LPs who commit liquidity for more extended periods, thereby ensuring the availability of durable depth to support cross-border settlement flows [21].

2.4.3 Canonical asset registry

To safeguard market efficiency and reduce systemic vulnerabilities, Gurufin governance maintains a

[27] Idle liquidity refers to funds locked in an Automated Market Maker (AMM) pool that are not actively used in trade execution because they are allocated outside the prevailing market price range, resulting in capital inefficiency.

Canonical Asset Registry [28] that designates authoritative representations of each currency admitted into the hub.

Without such coordination, liquidity for the same asset could be split across multiple representations, such as:

\ibc/<hash_uusdc>
(Stablecoin imported via IBC from Noble)

and

gwUSDC
(Token minted via the GatewayGX)

Resulting in liquidity fragmentation, this fragmentation weakens market depth, widens spreads, and forces arbitrage across parallel pools [1]. The registry addresses this by:

- Designating a canonical route for each asset, with preference given to IBC-based imports that preserve provenance and avoid bridge reliance.

- Recognising non-canonical routes (e.g., gateway-wrapped assets) only under governance-approved conditions and assigning them lower risk weights and transaction limits to reflect their higher exposure to bridge risk [2].

- Maintaining narrow-band (Figure 12) parity pools where both canonical and non-canonical routes are active, ensuring that prices remain aligned without forcing users into a single version.

This governance framework concentrates liquidity in the safest and most transparent channels, while preserving interoperability for legacy or non-IBC networks.

By mitigating liquidity fragmentation and controlling bridge risk, Gurufin strengthens its position as a neutral, resilient FX settlement hub.

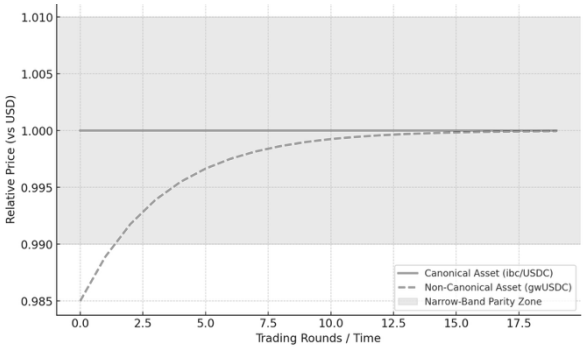


Figure 12 Narrow-Band Parity Pool Between Canonical And Non-Canonical Assets

2.5 Oracles & Arbitrage Automation (overview)

Gurufin Purpose is to ingest external price signals, including GXN/USD, fiat FX crosses, and benchmark market references to:

i. Keep Guru-PEG's fees predictable in fiat terms.

ii. Enable the paymaster to quote "all-in" cross-chain swaps in a single currency.

iii. Allow the *DexAggregator*[29] to align prices across AMM pools (Figure 13), RFQ venues, and parity pools, thereby compressing spreads without taking directional risk.

Gurufin's architecture works as a *permissioned provider*[30] set, comprising vetted exchanges, data firms, and institutional operators, that submits signed observations to Gurufin's on-chain *Oracle Module*.

The module enforces quorum rules, staleness bounds, and outlier filters, then aggregates inputs using robust statistical methods such as the weighted median [25]. This ensures resilience against manipulation and data faults while preserving accuracy.

All Oracle submissions and computed results are immutably recorded, enabling byte-for-byte recomputation for audit and supervisory review.

In parallel, arbitrage automation leverages these Oracle-verified prices to trigger routing through the

[28] The Canonical Asset Registry is a governance-maintained framework within Gurufin that designates the authoritative representation of each currency admitted into the hub, prioritizing IBC-native assets as canonical, while recognizing gateway-wrapped versions under lower risk weights and parity controls to prevent liquidity fragmentation.

[29] *A DexAggregator is a routing protocol that sources liquidity from multiple decentralized exchanges (DEXs) and automated market makers (AMMs), splitting or directing orders across venues to minimize slippage, optimize fees, and compress bid–ask spreads, thereby improving execution quality without taking directional market risk.*

[30] A permissioned provider is a pre-approved entity—such as an exchange, data service, or institutional operator—authorized by governance to submit signed observations to an Oracle module, subject to bonding, slashing, and quorum rules that enforce accountability and data integrity.

DexAggregator, which monitors AMM and RFQ venues.

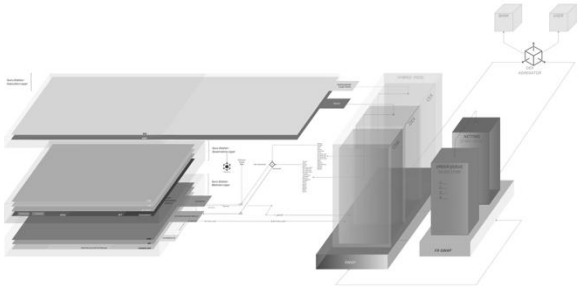


Figure 13 Neutral FX/DeFi hub - DexAggregator

By systematically exploiting price differentials across pools, the aggregator drives markets toward parity, compressing bid–ask spreads and ensuring efficient settlement conditions comparable to interbank FX[31] [26], [27], [28].

2.5.1 Oracle-dependent components

Guru-PEG (§4.2–§4.5): Guru-PEG reads GXN/USD to compute:

$$min\_gas\_price = gfiat/FX\{GXN/USD\}$$

(with congestion/circuit-breaker factors).

- Paymaster (§4.6): Paymaster uses fiat FX to settle multi-leg gas and relayers while charging the user in the source asset.

- DexAggregator: DexAggregator[32] compares pool mid-prices to a consolidated reference:

$$S = |(P\text{pool} - P\text{Oracle})/P\text{Oracle}|$$

- When the *relative spread* exceeds a governance threshold, it triggers neutral arbitrage (inventory-capped, rate-limited) to re-align markets[33].

- Resilience: The Oracle Module emits a degradation signal if feeds are stale or disagree beyond bounds, PEG/router enters deterministic degraded modes (freeze drift, conservative fallbacks; §4.5). Execution lanes reserve block capacity for Oracle and IBC traffic to preserve liveness.

2.5.2 Reference vs. executable pricing

Oracle FX feeds provide reference rates for fee normalization, quotes, and guardrails; the executable rate is discovered on the Station (AMM or RFQ).

Users receive a single, all-in quote denominated in the source asset, with min-receive and TTL[34]. The paymaster settles multi-leg fees and relayers under the hood using Oracle FX. Meanwhile, neutral arbitrage ensures that pool prices converge toward Oracle reference levels, compressing spreads within governance-defined bands.

If the Oracle feeds degrade or quorum fails, Gurufin transitions to a deterministic degraded mode in which quoting is based on fallback rules until data integrity is restored [28].

2.6 Privacy, compliance, and wallet-tier controls

2.6.1 Privacy – zkGuru

Applications can opt into selective-disclosure modes (e.g., hide amounts; hide amounts + recipient) under a standardized proving/verification service.

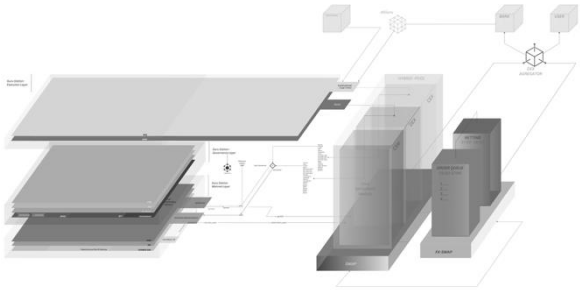


Figure 14 Neutral FX/DeFi hub - zkGuru

Personally identifiable information (PII) stays off-chain; view access for supervisors follows policy [29], [30].

Where required, selected adapters can run in Trusted Execution Environments (TEEs) with attestation; long-lived keys remain in HSMs [31], [32].

---

[31] Details as provider bonding/slashing, filters, failover are explained on §5.

[32] *§4.8*

[33] *Mechanics of the Oracle as provider sets, filters, failover are specified in §5; market-quality and representation-parity controls in §§4.8–4.9.*

[34] *In trading and settlement systems, Time-to-Live (TTL) specifies the maximum duration for which a quoted price or transaction instruction remains valid; if execution does not occur within the TTL window, the quote expires and the transaction is rejected to prevent stale or adverse fills.*

2.6.2 Wallet-tier compliance

KYC/AML, sanctions screening, Travel-Rule metadata, and per-wallet policy limits are enforced at the edge, keeping the base ledger simple while preserving supervisory auditability. When GX stablecoin rails participate, GX-style supervisory panels (e.g., reserve/flow telemetry) may be mirrored to uphold domestic oversight on a public hub [33], [34], [35], [36].

2.7 Security, keys, and upgrades

In Gurufin, validator operations and other critical services are secured through hardware-based and cryptographic safeguards. Key material is held in Hardware Security Modules (HSMs) or managed using Multi-Party Computation (MPC) schemes, with threshold signature controls ensuring that no single operator can unilaterally authorise sensitive actions.

Governance mandates rotation policies for operational keys and maintains break-glass procedures for emergency access under tightly controlled conditions[37], [38], [39].

Upgrades follow staged proposals with *Testnet* rehearsal and time-locked activation; jailing/slashing handle downtime and double-signing [40].

Standardised incident playbooks are published and distributed to participants, outlining coordinated recovery procedures for key compromise, consensus faults, or Oracle degradation.[41].

2.8 Economics and fees (architecture view)

Fees are engineered as narrow bands with governance-visible adjustments (e.g., CPI-indexed steps) so retail and institutional actors can budget *ex-ante*.

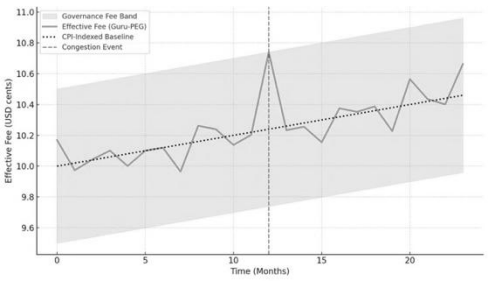


Figure 15 Narrow-Band Fee Design with CPI Indexing and Congestion Control.

Effective gas remains stable for users even under bursty load via Guru-PEG (fiat targeting), congestion multipliers (surge pricing), and lane isolation for system traffic (Oracle/IBC), as shown in Figure 16 [42], [43].

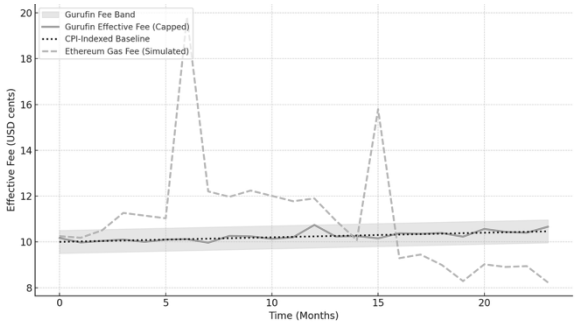


Figure 16 Gurufin Narrow-Band Fees Vs Ethereum Gas Volatility.

2.9 Relationship to GX stablecoin issuers

Jurisdiction-specific PoA (Proof of Authority) L1s (KRGX/JPGX/PHGX/USGX) handle local mint/burn, custody, and live proof-of-reserves.

Gurufin provides the neutral PvP FX fabric.
Interoperation uses policy-gated bridges (IBC/EVM).

When GX flows are involved, venue telemetry (depth, slippage, utilisation) can be mirrored for supervisory visibility, keeping issuance under domestic law while enabling global, 24/7 settlement on a public hub.

3. INTEROPERABILITY & SAFETY

3.1 Design Invariants

Gurufin's interoperability layer is built on a set of non-negotiable safety and liveness invariants:

Atomicity: All cross-chain settlements must resolve on a strict payment-versus-payment (PvP) basis, ensuring that no unilateral exposure to counterparty or bridge risk is possible.

Deterministic Finality: Cross-chain transactions achieve finality only when both source and destination chains provide cryptographic proof of settlement, minimizing replay or rollback risk.

Canonical Representation: For each supported asset, only one authoritative representation is recognized within Gurufin's canonical asset registry, preventing fragmentation and synthetic inflation.

Time-Bounded Resolution: All cross-chain messages must either complete within the specified timeout or automatically revert, ensuring resilience against censorship or message loss.

Supervisory Observability: All interoperability operations must be observable via verifiable telemetry and event logging, ensuring that supervisors and auditors can reconstruct decisions end-to-end.

3.2 Threat Model

The interoperability design explicitly defends against the following categories of technical and operational risk:

Finality Mismatches: Differing consensus assumptions across heterogeneous chains may cause temporary inconsistencies. Gurufin mitigates this through light client verification and finality thresholds that respect the weakest link.

Relayer Misbehavior or Censorship: Asymmetric control by relayers could delay or censor transactions. Gurufin enforces multi-party relayer redundancy, with penalty frameworks and timeout refunds to protect users.

Wrapped-Asset Inflation: Custodial bridges can issue non-canonical tokens without hard supply limits. Gurufin avoids this by prioritizing IBC-native channels and strictly governing gateway-issued representations with supply caps and transparent labeling.

MEV Exploits on Cross-Chain Transactions: Cross-domain transactions are vulnerable to frontrunning and reordering. Gurufin integrates batch auctions and intent-based RFQs to reduce exploitable surfaces.

Oracle Dependency Risk: Cross-chain settlement requires price and state validation. Gurufin relies on a permissioned oracle quorum with freshness, quorum, and outlier filters to minimize manipulation.

3.3 Controlled Extension via EVM Gateway

For networks that do not natively support IBC (e.g., Ethereum, Solana), Gurufin introduces an EVM gateway with controlled interoperability:

Dual control via oracle validation + timeout guarantees.

Strict supply limits on wrapped representations.

Clear governance rules distinguishing canonical vs. non-canonical routes.

Transparent asset labeling (e.g., gw* prefix) to ensure users and supervisors can distinguish gateway-issued assets.

4. GURU-PEG (PRICE EQUILIBRIUM GOVERNANCE): PRICE & FEE EQUILIBRIUM

4.1 Purpose

Guru-PEG ensures that end-user fees remain predictable in fiat terms, without targeting or defending any specific market price for GXN. Instead, the protocol adjusts the gas denomination so that each transaction reflects a stable, class-specific fiat fee [46].

≈ $0.013 for L1 sends

≈ $0.040 for asset/NFT

PEG consumes real-time GXN/USD from the decentralised Oracle set and updates the minimum gas price accordingly.

4.2 Fiat-fixed fee targeting

Let:

$$g\,fiat$$

Be the published fee target in USD (or the local-fiat equivalent displayed in the UI),

And:

FX_{GXN/USD}(*t*)

Be the Oracle price of 1 GXN in USD at time *t*.

i. Core rule

$$GasTarget_{GXN_{(t)}} = \frac{(g)fiat}{FX\left(\frac{GXN}{USD}\right)t}$$

ii. Initial fee classes

• L1 transfers:

$$gfiat^{L1} = 0.013$$

• Asset/NFT/complex ops:

$$gfiat^{Asset}=0.040$$

iii. CPI indexation: Governance may step *gfiat* on a fixed cadence (e.g., annually) in line with published CPI, subject to a per-step cap and advance notice, to support long-run sustainability and strong validator participation.

iv. Rounding & precision: Chain-level decimal precision and rounding policy are published ex-ante for wallet implementers.

4.3 On-chain integration

PEG writes the computed *min_gas_price* to the fee market so wallets/dApps automatically quote and pay gas at the updated GXN amount. The update path includes sanity bands (change-rate guards), peg buffers (± band around target), and failsafe floor/ceiling values for gas pricing.

4.4 Oracles for PEG

PEG relies on the network Oracle (§ 2.6) to fetch consolidated GXN/USD (and fiat FX where relevant).

Each request specifies period, quorum, approved providers, and aggregation rule (e.g., MEDIAN).

Submissions are validated on-chain; outliers are filtered; staleness windows and max-deviation triggers protect against manipulation.

4.5 Emergency & circuit breakers

Deterministic behaviour on a public chain: The PEG and fee-market modules operate as deterministic state machines driven entirely by on-chain data; there are no manual switches.

Normal mode: The chain computes

$$\min_{\text{gas}_{\text{price}}} = \frac{gfiat}{FX\left(\frac{GXN}{USD}\right)}$$

And publishes it to the fee-market[35].

Degraded mode: If Oracle inputs become stale (beyond a configured staleness window) or diverge (beyond a configured deviation band), the module freezes drift and applies a conservative fallback:

$$\text{min\_gas\_price} = \max\left(\text{last}_{\text{good}}, \text{fallback}_{\text{floor}}\right)$$

Enable an Oracle-risk multiplier.

$$m\text{Oracle} \geq 1$$

So, an effective gas cannot collapse during uncertainty emit on-chain events (mode change, reason, timestamps).

Auto-recovery: When Oracle Health returns within bounds for a required number of consecutive updates, the module exits Degraded mode and resumes Normal computation.

Congestion awareness: To resist spam under pegged fees, the effective base fee multiplies by a load factor:

$$min_{gas_{price_{(t)}}} = \frac{g_{fiat}}{FX\left(\frac{GXN}{USD}\right)(t) * m\text{load}(t) * m\text{Oracle}(t)}$$

Here, the mload(t) increases as block utilisation exceeds a target range and decreases when load lessens, within set caps. This maintains a fiat-like user experience in calm periods but makes sustained spam economically expensive [47], [48], [49].

Queue isolation for liveness: Execution lanes reserve capacity for IBC system messages, Oracle submissions, and governance, distinct from the general user lane [50].

Lane reserves and distinct minimums ensure cross-chain settlement and price feeds remain live during user-traffic spikes [51], [52].

Governance posture and disclosure: Parameter categories, such as staleness windows, deviation bands, fallback floors, surge caps, and lane reserves, are governed *on-chain* with a Timelock and surfaced via public telemetry. Exact production thresholds are maintained in operational documentation and may evolve with network conditions.

4.6 "All-in" fee experience (sponsored FX swaps)

For cross-chain stablecoin PvP (e.g., USGX → KRGX), users may pay entirely in the source asset. A paymaster sponsors the Gurufin leg (GXN gas via PEG) and prefunds IBC relayers, then nets costs inside the quote.

Typical legs:

- Source GX Stablecoin Chains fee (≈ $0.013 or local-fiat target)
- Neutral FX/DeFi hub fee (≈ $0.013 via PEG),
- Destination GX Stablecoin Chains fee (≈ ₩20 ≈ $0.013)
- Two small relayer fees
- Stable-swap pool fee (2–5 bps)

PEG guarantees the GXN portion equals the published fiat target at execution time; any FX conversion is handled by the paymaster with a short TTL and buffer, and unused buffer is auto refunded.

[35] §4.2

4.7 Execution fabric (stable-swap AMM + RFQ)

Flow types: The Station optimises for stablecoin to stablecoin and stablecoin to GXN flow, supporting same-chain execution when both representations are resident on Gurufin as IBC vouchers, enabling a single-transaction atomic swap and cross-chain payment-versus-payment (PvP) when assets live on different ledgers, using escrowed holds and IBC delivery so neither leg completes unless both do.

Routing primitives: Gurufin integrates stable-swap CFMMs for near-par stablecoin execution, RFQ paths for large trades with minimal slippage, and TWAP/TWAMM slicing to handle very large or time-sensitive orders with reduced market impact.

- Stable-swap CFMMs (*Constant-Function Market Maker*) with low curvature and an amplification parameter, a per pair class for near-par execution on correlated assets.

- RFQ paths for size on off-chain quote formation with on-chain settlement, minimising slippage for large tickets.

- TWAP (*Time-Weighted Average Price*)/TWAMM (*Time-Weighted Automated Market Maker*) slicing for very large or time-sensitive orders to reduce market footprint.

Settlement paths and fees: Same-chain swaps settle atomically on Gurufin with only the Neutral FX/DeFi hub fee. Cross-chain PvP swaps include local PoA fees at source and destination, relayer incentives for IBC packets, and the Neutral FX/DeFi hub fee. Wallets display a single fiat-quoted total, with paymasters able to sponsor GXN legs and net costs.

- *Same-chain swap (on Gurufin):* Atomic execution at the DEX layer; the user pays the Neutral FX/DeFi hub fee only.

  ≈ $0.013 in GXN
  amount sized by PEG

- *Cross-chain PvP swap*

  USGX → KRGX

- Source GX PoA chain escrows or burns the source asset and charges its local fee target.

- IBC packet to Gurufin (relayer incentive).

- Atomic swap on Gurufin (Neutral FX/DeFi hub fee ≈ $0.013 in GXN via PEG).

- IBC packet to destination (relayer incentive).

- Destination GX PoA chain mints or releases the asset and charges its local fee target.

Wallets may present a single, fiat-quoted total; a paymaster can sponsor the GXN leg and relayers, netting costs in the quote and refunding any buffer.

Gas abstraction & UX: Users can pay in the source asset; the paymaster converts under the hood, preserving PvP atomic safety with predictable checkout.

4.8 Market quality: AMM + RFQ + neutral arbitrage

The Neutral FX/DeFi hub combines stable-swap CFMMs for correlated pairs with RFQ paths for size.

A *DexAggregator* monitors the Neutral FX/DeFi hub pools and sister venues, compares mid-prices to Oracle references, and triggers neutral arbitrage when the relative spread exceeds a governance threshold *Strig*:

$$S = \left|\left(\frac{P_{pool} - P_{oracle}}{P_{oracle}}\right)\right|$$

Keepers are route-neutral, inventory-capped, and rate-limited to tighten spreads without directional risk. Safety rails pause or widen limits when reference feeds are stale or disagree beyond maximum deviation bands; governance parameters include:

- *S*trig,
- Keeper budgets.
- Kepper velocity caps.
- Reporting cadence.

4.9 Representation parity (IBC vs. gateway)

If multiple representations of the same currency exist (e.g., USDC via IBC and USDC via a gateway), governance:

Designates a canonical route (prefer IBC where available) and publishes denom provenance (origin chain, channel/contract).

Optionally operates a small, capped parity pool to keep a narrow basis:

$$\left|\left(\frac{P_{gw} - P_{ibc}}{P_{ibc}}\right)\right| \leq \delta_{parity}$$

De-prioritises or auto-halts non-canonical routes if the basis or Oracle disagreement exceeds hard bands.

All choices are mirrored in the canonical asset registry to prevent liquidity fragmentation.

4.10 Liquidity programs

- Fee tiers by pair class (stable-stable, stable-GXN, long-tail).
- Bonded liquidity. Time- LP positions receive:
    - Boosts.
    - Early-exit penalties feed a safety buffer.
- Inventory bands & LP caps to avoid concentration.

Emission schedules and pool-class tiers are set in *Tokenomics*.

4.11 MEV & execution protections

- Frequent batch auctions or intent/RFQ for size to curb sandwiching.
- Volatility guards that widen slippage ceilings or throttle large orders when realised volatility breaches pair-class thresholds.
- Min-receive enforced on-chain to respect user slippage.

4.12 Telemetry & disclosures (public by default)

- Fee telemetry: target vs. realised (in fiat), CPI steps, any controller adjustments.
- Market telemetry: pool depth, realised slippage, utilisation heatmaps.
- Stability metrics: parity basis, Oracle disagreement, arb latency, halt events.
- Route registry: canonical/non-canonical flags, caps, and state (active/paused/deprecated).
- All feeds are machine-readable; summarised dashboards are available for users and supervisors.

4.13 Initial parameter slate (Testnet, to be finalised)

Parameter	*Purpose*	*Testnet default*
$gfiat^{L1}$	L1 fee target	$0.013
$gfiat^{Asset}$	Asset/NFT fee target	$0.040
CPI cadence	Indexation interval	Annual (or quarterly)
CPI cap	Max step per update	≤ 2% per step
Fee band	Guardrails around target	± 5%
A (CFMM amp)	Stable-swap curvature	100–500 (by pair class)
***S*trig**	Arbitrage trigger	10 bps
δ_{parity}	Parity basis band (IBC vs gateway)	10 bps
τ_{max}	Oracle staleness window	60 s
Rounding	Gas rounding policy	6–18 decimals (publish exact)

∗36

Key takeaway: Guru-PEG makes fees feel like fiat, with fees of about $0.013 for simple transfers and $0.040 for asset operations, by adjusting the GXN amount per transaction as GXN's market price moves.

Tight execution comes from stable-swap AMMs + RFQ, neutral arbitrage, and parity management where multiple representations exist. Oracles, CPI indexation, and full telemetry keep the system observable, governable, and predictable.

5. ORACLE NETWORK & DATA INTEGRITY

The Guru Oracle Network underpins Gurufin's settlement infrastructure by delivering trusted, tamper-resistant market data to protocol modules.

Price observations are sourced from permissioned reporters, including exchanges, data providers, and community operators, who submit signed values under governance-set quorum, staleness, and outlier constraints.

Equation 1 Weighted arithmetic mean

$$\bar{x} = \frac{\sum_{i=1}^{n} w_i x_i}{\sum_{i=1}^{n} w_i}$$

Aggregation relies on robust statistics (weighted median by default, Equation 1) to resist manipulation, while every accept, reject, and aggregate step is immutably recorded for byte-for-byte recomputation.

[36] Note: Values are indicative and may differ by network (testnet/mainnet), corridor, or pair class. Exact thresholds are governed on-chain with *Timelock* and disclosed via the public parameter registry and telemetry.

This architecture ensures data integrity, auditability, and supervisory visibility, aligning Oracle performance with financial-market standards of transparency and reliability.

5.1 Objectives

The Oracle layer supplies authoritative signals to the GXN/USD protocol for Guru-PEG, fiat FX and for paymaster conversions, stablecoin parities, and market reference prices routing and neutral arbitrage. It is designed around three invariants:

1. Robustness (resistant to bad ticks/outliers).
2. Liveness (fresh values under stress).
3. Auditability (provable provenance and reproducibility).

5.2 Data model (feeds)

Core feeds include:

i. GXN/USD.
ii. Fiat FX crosses (USD/KRW, USD/JPY) with a consistent triangulation matrix.
iii. Stablecoin references (USGX/USD ≈ 1, KRGX/KRW ≈ 1).
iv. Venue mid-prices for listed assets used in routing sanity checks.
v. Low-frequency CPI index points for fee indexation.

Each feed is a time-stamped tuple ⟨value, variance proxy, sample count, window⟩ with signed provider metadata.

5.3 Architecture

Reporters (exchanges, market data firms, and permissioned community operators) submit signed observations to an on-chain Oracle Module. The module enforces per-feed quorum, staleness constraints, and outlier filtering, then computes an aggregate using robust statistics (weighted median by default).

Every step (accept/reject/aggregate) is recorded in state to enable byte-for-byte recomputation from raw submissions.

5.3.1 Weighted Median in Oracle Aggregation

Suppose the Gurufin Oracle Module is collecting USGX/USD exchange rate observations. Five permissioned reporters submit the following signed values (fees):

A: 1.0001 Exchange
B: 1.0003 Data Firm
C: 0.9998 Exchange
D: 1.0500 (outlier)
E: 1.0002 Community Operator

Step 1 Validation: The module checks each submission against quorum rules, staleness bounds, and outlier filters. Exchange D's value (1.0500) is rejected as an outlier.

Step 2 Weighted Median: Each reporter is assigned a *Governance-Set Weight,* and the accepted submissions are arranged in ascending order by their value:

C: 0.9998 Exchange	25%
A: 1.0001 Exchange	30%
E: 1.0002 Community Operator	15%
B: 1.0003 Data Firm	30%

Then, a calculation of the cumulative weight is done by adding the weights sequentially. The weighted median is the first value in the ordered list where the cumulative weight- Σwm (Past value + Present Value) is equal to or greater than 50%:

C: 0.9998	25%	Σwm	0.25<0.50
A: 1.0001	30%	Σwm	0.55>0.50
E: 1.0002	15%	Σwm	0.70>0.50
B: 1.0003	30%	Σwm	1.00>0.50

Step 3 Recording: The raw submissions, accepted set, and the final aggregate are written to the chain state. This enables supervisors to recompute byte-for-byte the Oracle decision if challenged.

The resulting rate (1.0001) is fed into Guru-PEG for fiat fee sizing and into routing guardrails for corridor execution, ensuring that fees remain predictable and markets align with consensus-validated data.

5.4 Provider set, bonds, and incentives

i. Providers register with a bond in GXN and a published key.
ii. Rewards accrue per accepted submission.
iii. Misbehaviour is *slashable* with graduated penalties:

- Repeated stale reporting.
- Extreme deviations without market corroboration.
- Equivocation.

warning → partial slash → ejection

iv. A public quality score weights provider influence within bounded ranges to avoid cartelization:

- Coverage.
- Timeliness.
- Deviation history.

5.5 Aggregation & filters

Given provider values:

$$p_1, \ldots, p_n$$

Arriving within window *W*:

Pre-filters: Discard submissions with

$$age > \tau\_max$$

or,

Without sufficient venue depth (for VWAP providers).

Outlier screen: Compute preliminary median:

$$p\sim$$

Reject any:

$$p\text{i}$$

With

$$\frac{|p_i - p\sim|}{p\sim} > \Delta\text{max}$$

Aggregate: weighted median (primary) or trimmed mean (fallback), with weights derived from provider quality and venue diversity.

Triangulation checks: Enforce loop consistency (Violations trigger soft rejections or variance inflation).

$$\left(\frac{USD}{KRW}\right) * \left(\frac{KRW}{EUR}\right) * \left(\frac{EUR}{USD}\right) \approx 1 \cap \varepsilon$$

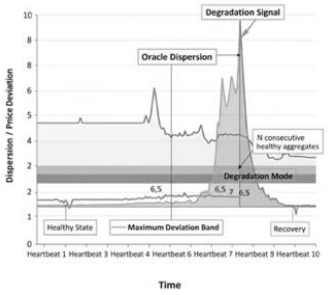
∗[37]

The module also compares the aggregate to station pool references and flags deviations to the *DexAggregator* for neutral arbitrage, without letting pool prices "pull" the Oracle.

5.6 Liveness & failover

Feeds run on explicit heartbeats:

1–5 s for GXN/USD



Time (Heartbeat)	Oracle Dispersion / Price Deviation ~
1	~1.5
2	~1.5
3	~2.0
4	~8.0
5	~7.0
6	~7.0
7	~6.5
8	~2.0
9	~1.5

Figure 17 Oracle Liveness and Failover

Tens of seconds for fiat FX, with grace windows and provider rotation. If a live quorum fails or dispersion breaches a maximum deviation band, as it is expressed in Figure 18, the module emits a degradation signal.

Protocols that consume the Oracle (Guru-PEG, router) then enter their deterministic degraded modes (freeze drift, conservative fallbacks[38]. Recovery requires N consecutive healthy aggregates.

5.7 Security posture

Provider keys are HSM-guarded; rotation requires on-chain notice and cooldown. Optional TEE attestations [39] can accompany submissions for operators that support enclave execution [31].

Remote Procedure Call [40] (RPC) ingestion is rate-limited and Denial of Service [41] (DoS) scored; duplicate or malformed payloads are dropped at the gateway.

All provider actions and Oracle decisions are indexed for audit [53].

[37] ∩ ε =Within ε.

[38] §4.5

[39] *T*rusted Execution Environment (TEE) attestation is a cryptographic protocol by which a TEE produces a verifiable proof—signed by hardware-backed keys—that specific code executed within the enclave with integrity and confidentiality guarantees, enabling remote parties to trust the enclave's state without direct access.

[40] Remote Procedure Call (RPC) is a communication protocol that allows a program to request a service or transmit data to a remote server or node as if it were a local procedure call. In blockchain systems, RPC endpoints serve as the interface through which clients submit transactions, query state, or relay external data.

[41] A Denial-of-Service (DoS) attack is a disruption method in which an adversary overwhelms a target system with excessive or malformed requests, degrading or preventing normal service availability. In distributed networks, DoS protections include rate limiting, scoring, and filtering mechanisms at ingestion points.

5.8 Transparency & auditability

For each aggregate, the chain stores:

- Provider list
- Raw values
- Acceptance masks
- Chosen estimator
- Final value with variance proxy.

Off-chain archives retain source venue IDs and sample windows for providers that compute VWAPs[42].

A machine-readable feed exposes ticks, health, staleness, dispersion, and triangulation residuals in real time, enabling supervisors and integrators to validate behaviour [54].

5.9 Consumption by protocol

Guru-PEG reads:

GXN/USD

And writes:

$$min_{gas\_price} = \frac{g_{fiat}}{FX\left\{\frac{GXN}{USD}\right\}}$$

Subject to load multipliers and circuit breakers[43].

Paymaster: uses fiat FX to convert source-asset payments into destination legs and GXN fees, with a short TTL and buffer.

DexAggregator: Monitors Oracle vs pool spreads.

if

$$\frac{|\ P_{pool} - P_{ref}\ |}{P_{ref}} > S_{trig}$$

Where:

P_{pool} = price implied by the Gurufin liquidity pool.
P_{ref} = reference price from the Oracle (weighted median, VWAP, etc.).
S_{trig} = governance-set trigger value

It schedules neutral arbs (inventory-capped, rate-limited)[44].

5.10 Initial parameters (illustrative; governed)

Exact values are set by governance with Timelock and disclosed via the parameter registry; operations guides maintain runbooks and alarms. *Staleness windows*:

- Fast feeds 30 – 60 s.
- fiat FX 60 –
- 180 s.

Max deviation band (per burst):

- 25–50 bps before degradation signal.

Quorum:

- *≥ 5 providers.*
- supermajority of independent sources.

Estimator:

- Weighted median (primary).
- 20% trimmed mean (fallback).

Slashing tiers:

- Warning → 0.5–2%.
- Bond → ejection for repeat offenders.

6. LIQUIDITY LAYER & MARKET STRUCTURE

6.1 Objectives

The Station's liquidity layer must deliver tight spreads, predictable execution, and PvP-safe settlement across heterogeneous assets and routes (IBC and EVM).
It reconciles two realities; the most real-world flow is:

stablecoin↔stablecoin

or

stablecoin↔GXN

Yet assets can arrive via different provenance paths. Market quality is achieved by combining stable↔swap AMMs for correlated pairs, RFQ for size, neutral arbitrage to remove residual basis, and a canonical asset registry to prevent fragmentation.

---

[42] The Volume-Weighted Average Price (VWAP) is a trading benchmark that represents the average price of an asset over a specified time window, weighted by trade volume. VWAP is calculated as the ratio of the cumulative traded value ($\sum P_i \times V_i \backslash sum\ P_i \backslash times\ V_i \sum P_i \times V_i$) to the cumulative traded volume ($\sum V_i \backslash sum\ V_i \sum V\hat{i}$), and is widely used for execution quality measurement, trading strategy benchmarks, and Oracle data aggregation.

[43] §4.2–§4.5.

[44] §4.8

6.2 Asset representations and the canonical registry

Assets enter Gurufin by two paths, IBC assets are represented natively as:

ibc/<hash> (ICS-20).

Non-IBC assets are minted by the EVM gateway under a separate namespace on *TokenFactory* following the CW-20 protocol and exposed in UX with the symbols:

*gw**

To avoid split liquidity and ambiguity, governance maintains a canonical asset registry mapping symbols to their authoritative representation, origin, and limits.

Operators and venues must display the exact on-chain denom in settlement, while user-facing symbols remain consistent across the ecosystem.

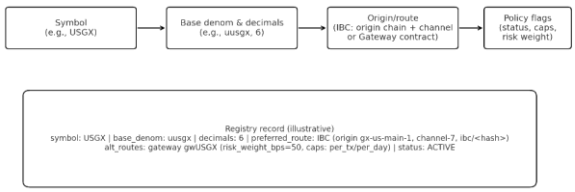


Figure 18 Canonical asset registry

6.3 Pool topology

Foundational pools ("CSM [45] pools") pair each canonical stablecoin with GXN to unify accounting across routes, for example:

ibc/<hash_uusgx> ↔ GXN

ibc/<hash_uusdc> ↔ GXN

and (where enabled):

gwUSDC ↔ GXN

When depth, provenance, and risk criteria are met, direct pools such as:

stable↔stable

ibc/<hash_uusgx> ↔ ibc/<hash_ukrgx>

They are activated to minimise intermediate exposure and reduce slippage for FX-like trades. If multiple representations of "the same" currency coexist, a narrow-band parity pool may be enabled to keep prices aligned while still signalling route quality via the registry [55], [56].

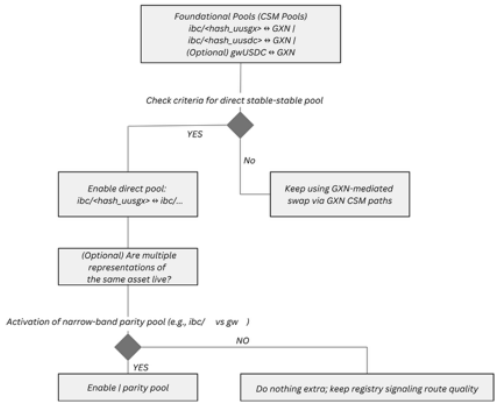


Figure 19 AMM design for correlated pairs

6.4 AMM design for correlated pairs

Correlated pairs use a stable↔swap constant-function with low curvature near parity. An amplification parameter [46] AAA (governance-set by pair class) flattens the invariant around the peg, yielding lower slippage for modest imbalances [57].

The invariant and fee policy are published, calibration balances:

i. Slippage near 1:1.
ii. Resilience to inventory shocks.
iii. Predictable LP returns.

Fee proceeds are split between LPs and the protocol as specified in Tokenomics.

6.5 RFQ for size and discretion

For large or institutionally quoted tickets, venues can route to RFQ makers. Quotes are collected off-chain with expiry Time to Live (TTL) and settle on-chain atomically. RFQ paths reduce price impact, respect client min-receive terms, and enable makers to hedge across venues. Quotes may incorporate all legs:

- Source
- Station
- Destination
- Relayers

[45] Cosmos-native Settlement Module.

[46] The amplification parameter (A) is a tuning constant in stable-swap Automated Market Makers (AMMs) that adjusts the curvature of the constant-function invariant near the peg. Higher values of A flatten the bonding curve around parity, allowing the pool to mimic higher liquidity depth and thereby reduce slippage for trades involving modest imbalances between correlated assets (e.g., stablecoins), while still reverting to a constant-product profile under extreme imbalance.

Thus, counterparties see a single executable price.

6.6 Routing and execution safety

Same-chain swaps (when both representations are resident on Gurufin) clear atomically in a single transaction.

Cross-chain swaps settle payment-versus-payment (PvP):

- The source chain escrows leg-A
- Gurufin executes the exchange
- Destination chain releases leg-B only when the escrow proofs are complete.

Escrows use IBC timeouts/holds; neither leg completes unless both do. Users see one all-in quote; the paymaster abstracts gas and relayer micro-fees.

6.7 Neutral arbitrage and basis control

A DexAggregator continuously compares pool mid-prices to a consolidated price. Oracle reference. When the relative spread:

$$S = \left| \frac{P_{pool} - P_{ref}}{P_{ref}} \right|$$

Exceeds the governance threshold *S*trig, the protocol (and permissionless keepers under identical limits) executes route-neutral, inventory-capped trades to re-anchor prices.

Under Oracle degradation, arb velocity tapers automatically. This mechanism tightens spreads without taking directional risk or privileging any venue.

6.8 MEV and execution protections

The router mitigates common MEV vectors by:

(i) Supporting frequent-batch execution for bursts.
(ii) Honouring user min-receive strictly on-chain.
(iii) Preferring intent/RFQ for size to reduce sandwich surface.
(iv) Applying volatility guards that widen slippage ceilings or throttle block-share during shocks.

Observability includes realised slippage and sandwich detection statistics.

6.9 Liquidity programs and incentives

Depth is encouraged via programmatic incentives. Pools are tiered by pair class, each with fee bands and reward schedules.

stable↔stable

stable↔GXN

long tail

Bonded liquidity (time-locked LP positions) can earn boosts; early exits route penalties to a safety buffer.

Inventory bands, LP caps, and route-specific risk weights prevent concentration and reflect provenance quality:

IBC canonical > gateway

6.10 Fees and economics (market layer)

Swap fees are lean and transparent, with a typical starting grid:

- 2–5 bps for stable↔stable
- 5–10 bps for stable↔GXN

And higher for volatile pairs, subject to governance. The Neutral FX/DeFi hub gas is fiat-fixed via Guru-PEG[47]; the paymaster can bundle the three protocol legs:

- Source L1.
- Station.
- Destination L1.

And two tiny relayer fees into a single user-quoted total. Fee flows and splits (LPs vs protocol) are reported per-pool.

6.11 Telemetry and supervisory visibility

All venues publish machine-readable telemetry:

- Pool depth
- Utilisation
- Realised slippage
- Deviation vs Oracle reference.

Gurufin mirrors these to public dashboards and, where GX flows are involved, to supervisory views compatible with GX Guru Scanner conventions.

Canonical/alternate route states:

- Active.

[47] §4

- Paused.
- Deprecated.

Are openly reported.

6.12 Initial parameters (illustrative; governed)

Amplification A by pair class:

100–500 for stable↔stable

Strig = 10 bps default, parity-basis band:

δparity = 10 bps

Maker TTLs of:

30–60 s.

Governance may be refined via time-locked updates; parameter histories are archived for audit.

7. SECURITY, VALIDATORS & UPGRADES

7.1 Security objectives

Gurufin targets four invariants:

i. Safety (no equivocation or state forks after finality)
ii. Liveness (progress under partial faults)
iii. Integrity (tamper-evident audit trail)
iv. Operational resilience (fault isolation, rapid recovery).

Controls span cryptography (HSM/MPC), network design (sentries, rate-limits), economics (slashing), and process (staged upgrades, timelocks).

7.2 Validator set & staking (DPoS)

Delegated Proof-of-Stake (DPoS) Mode: Token holders delegate GXN to validators; stake-weighted selection, with caps to reduce concentration:

cap 10–12% per operator

Set size: Target active set $N \approx 100–150$. Governance may adjust with demand and latency budgets.

Key management: Consensus and signing keys are HSM-guarded (or MPC), with rotation policies and break-glass[48] procedures under dual control.

Sentry architecture: Public sentries shield validator cores; cores are firewalled and privately peered. DDoS is absorbed at sentry layer; per-IP/ASN rate-limits apply[58].
Slashing & jailing. Double-signing and prolonged downtime result in jail. Un-jailing requires liveness proofs; repeat offenders face extended quarantines.

Relayer quality: IBC relayers run with per-channel budgets and proof-of-work attestations for spam control; a light incentive and reputation score are published by the Indexer.

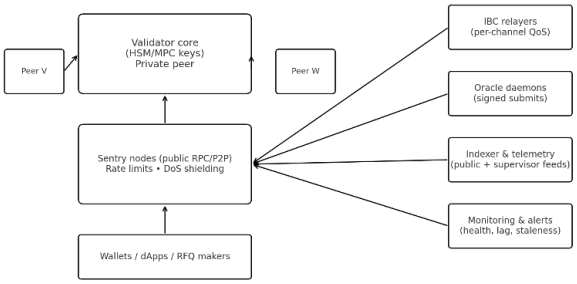


Figure 20 Validator & sentry architecture

7.3 Finality, latency & throughput

Consensus: TBFT (Tendermint Byzantine Fault Tolerance) with fast-finality with a Block time target:

2.5~3.0s.

Execution: Deterministic Application Blockchain Interface [49] (ABCI) execution with Mempool admission guards; parallelisation for non-conflicting TX classes is on the roadmap.

Design targets: Retail confirmations:

< 800 ms on-chain acceptance

< 2–3 s finality.

Sustained TPS: 2–5k stable-swap/transfer-heavy mixes on commodity validators; burst handling via queueing and fee bands [59].

[48] A break-glass procedure is an emergency access mechanism that bypasses normal security controls to allow critical operations (such as key recovery or system override) in exceptional circumstances. Break-glass access is typically subject to dual control, strict auditing, and immediate post-event review to prevent misuse while ensuring system continuity.

[49] The Application Blockchain Interface (ABCI) is a generic interface that connects a Byzantine Fault Tolerant (BFT) consensus engine, such as Tendermint Core, with the application state machine. ABCI enables deterministic transaction execution across all by separating consensus (ordering and finality) from application logic (state transitions), thereby supporting modular blockchain architectures.

Benchmarking method:

- Open/closed-loop harness.
- Zipfian TX mix (transfers, swaps, IBC sends).
- Cold/warm cache runs.
- WAN latency injected.
- Report p50/p95/p99 latency.
- CPU/IO headroom.
- Reorg rate (0 at finality).

7.4 Fee-market hardening & anti-spam

Fiat-fixed base fee: Guru-PEG sets *min_gas_price* in GXN to meet fiat targets[50]; a floor prevents zero-fee spam, and a band (+/−%) absorbs short spikes.

Admission & QoS: Mempool uses priority buckets per-sender rate-limits, and stake/identity weighting for service fairness:

- BC
- Oracle
- Consensus-critical lanes reserved

Circuit-breakers: In response to Oracle degradation or suspected L7 attacks, the chain transitions into a deterministic degraded mode, characterised by freezing PEG drift, tightening mempool, throttling large swaps, and preserving headroom for IBC/Oracle packets (§4.5).

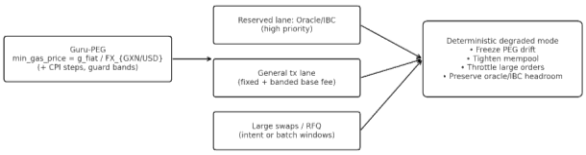


Figure 21 Fee market & QoS lanes (Guru-PEG + degraded mode)

7.5 MEV & execution protections

Strict min-receive on swaps; intents/RFQ for size; optional frequent batch auctions during bursts.

Observability: Indexer publishes realised slippage, *sandwich* detection, and latency histograms; governance can enable mitigations per-pair:

- Batch
- Windows

7.6 Upgrades & parameter governance

Time-locked governance: All parameter changes and code upgrades follow a proposal:

→ *vote* → *Timelock* → *enact.*

Emergency changes have narrower windows but require a higher quorum and multi-sig attestations.

Staged releases: Canary Testnet → shadow Mainnet (read-only) → phased activation with rollback points (Figure 23).

Data migrations are idempotent and checkpointed.

Parameter registry: A machine-readable on-chain registry exposes active values:

- *A* for CFMMs.
- *S*trig for arbitrage,
- PEG bands.
- CPI step.

With full version history for audit.

7.7 Monitoring, incident response & audit

Monitoring: Validators and core services export health (CPU, peer count, gossip lag), Mempool depth, IBC backlog, Oracle staleness, and PEG variance. Threshold breaches trigger alerts.

Incident playbooks: Published runbooks for fork detection, relayer congestion, Oracle degradation, and large-ticket throttling. Drills are scheduled and logged.

Audit trail & Immutable logs: proposal history, parameter diffs, Oracle aggregates (raw + filtered), and keeper actions. Periodic third-party audits are published with remediation timelines.

7.8 Interop safety (IBC & gateways)

IBC channels: Canonical channels per asset/pair; packet filtering, timeouts, and proof verification enforced.

Channel changes require governance notice and grace periods.

Gateways: Non-IBC routes are sandboxed, and optional parity pools keep non-canonical representations aligned without forcing users into one venue.

- Per-route caps
- Risk weights

[50] §4

8. COMPLIANCE, PRIVACY & OPTIONAL COMPLIANCE HOOKS

8.1 Objectives and stance

Gurufin is a public, permissionless DPoS network.

The protocol's stance is:

Comply where required, permit where allowed.

Issuance, redemption, and other sovereign obligations remain on jurisdictional rails under domestic law.

Jurisdictional PoA L1s (KRGX/JPGX/PHGX/USGX)

Gurufin provides neutral, PvP settlement for cross-currency flows.

Personally identifiable information (PII) is kept off-chain; the chain enforces behavior through verifiable proofs, policy flags, and audit-ready events rather than storing identity data.

8.2 Wallets & identity proofs (non-custodial by default)

Guru Wallet is non-custodial: Users hold their own keys; the wallet does not take possession of funds and is designed to operate without acting as a custodian/VASP.

When a regulated corridor or asset demands eligibility, any compatible wallet (including Guru Wallet) can obtain verifiable credentials (e.g., W3C VC/DID) from independent providers and present cryptographic proofs of attributes:

- Residency
- Sanctions "no-hit as of t"
- Risk tier.
- Policy limits.

Proofs are checked on-chain; raw KYC data never is designation as a VASP[51], if any, depends on local law and the totality of services offered.)

8.3 Transaction-time policy checks (applied only where required)

Regulated corridors declare their rule sets on-chain:

- Thresholds.
- Allow/deny lists.
- Credential requirements.

At execution:

Inputs:

- Credential proofs (not PII).
- Corridor code.
- Asset/amount.
- Optional Travel-Rule commitment reference.

Engine: Deterministic allow/deny with reason codes:

- Sanctions_hit.
- Limit_exceeded.
- Corridor_requires_vasp.
- Proof_stale.

Per-wallet caps and velocity guards are enforced before execution.

Liveness: Green paths use short-TTL caches; proofs have freshness windows:

$$sanctions \leq 24h$$

If policy sources are unavailable, corridors fall back to deny or reduced limits (governed), without halting the chain.

Permissionless venues continue to operate with no credential checks.

8.4 Optional compliance hooks (Travel Rule & VASP interoperability)

Where applicable law requires the Travel Rule (typically VASP↔VASP flows), Gurufin exposes minimal hooks:

Off-chain envelope: IVMS-101-class payload exchanged off-chain between VASPs [52] or via a recognised TR network [60], [61].

On-chain anchor: the transaction carries a commitment hash and delivery-receipt proof; the chain verifies presence/freshness, not contents.

[51] A VASP is a regulated business that deals in the exchange, transfer, or custody of virtual assets, falling under FATF standards for AML/KYC and Travel Rule compliance.

[52] *IVMS 101*: The interVASP Messaging Standard 101 (IVMS 101) is a data model that serves as a universal common language for Virtual Asset Service Providers (VASPs) to securely exchange customer data in compliance with the FATF's "Travel Rule" for virtual asset transfers.

Self-custody paths: allowed only if the corridor's policy permits credentialed self-custody; otherwise denied with a reason code.

Detailed VASP playbooks remain out of scope for the core protocol and are documented separately for regulated partners.

8.5 Privacy modes (zk-assisted, supervisor-auditable)

Gurufin offers optional, opt-in privacy for commercial use cases while preserving permissionless access and supervisory audit.

Mode 0 (public-default): sender, receiver, and amount are visible on-chain.

Mode 1 (amount-confidential): the amount is hidden using zero-knowledge range proofs; sender and receiver remain public.

Mode 2 (selective disclosure): amount and/or counterparty are concealed from the public; authorised reviewers can decrypt via view keys furnished by the user under lawful process.

Access grants are logged immutably.

Deterministic compliance: In all modes, policy checks (sanctions/no-hit proofs, per-wallet limits, Travel-Rule presence where applicable) are enforced before execution using verifiable proofs; no PII is stored on-chain.

Implementation notes: Privacy is delivered via ZK shielded pools (commitments + proofs) and, where required, TEE-assisted adapters for specific edges. Both are off by default and enabled per asset/corridor and jurisdiction.

A dedicated "zkGuru" specification will detail circuits, viewing policies, and auditor-key management.

8.6 TEEs at the edge (optional)

Selected adapters (e.g., paymasters, institutional gateways) may run in Trusted Execution Environments (TEEs) with remote attestation recorded on-chain.

TEEs protect ephemeral secrets and in-process data; long-lived keys stay in HSMs. This offers higher assurance without obscuring protocol behaviour.

8.7 Data boundaries, retention, and auditability

On-chain: policy decisions (allow/deny + reason), proof commitments, Travel-Rule commitment/receipt status, corridor policy versions, and non-PII telemetry. *Off-chain*: KYC evidence and full Travel-Rule payloads retained by the responsible verifiers/VASPs under local law.

Audit: supervisors can reconstruct decisions end-to-end using on-chain logs plus off-chain records; all Oracle/policy changes are parameter-registered with diffs and timestamps.

8.8 Observability & supervisory mirroring

Public dashboards and machine-readable feeds expose:

- Corridor utilisation.
- Policy hit-rates.
- Oracle health and staleness.
- PvP settlement integrity.
- When GX rails participate.
- Mirrored reserve/flow.
- Panels from GX scanners.

Supervisor-console access is read-only, key-scoped, and fully logged; exports are watermarked and hash-anchored for provenance.

8.9 Incident response (policy layer)

On detected breach or emergency bulletin:

i. *Contain*: Freeze the credential or corridor at the wallet/policy layer (deny new transfers; allow redemptions if law permits).

ii. *Signal*: Emit an on-chain incident code (non-PII) and raise alerts.

iii. *Coordinate*: Originating/beneficiary providers exchange off-chain case references; supervisors notified automatically.

iv. *Restore*: Resume after credential refresh or parameter update; publish a post-incident record via the parameter registry.

8.10 Governance parameters (Illustrative: Set by vote & *timelock*)

Gurufin keeps the base chain permissionless and open, adds opt-in proofs and minimal hooks where laws

demand them, and ensures privacy features remain compatible with supervisory audit.

Compliance happens at the edge; the ledger remains a neutral, high-assurance settlement fabric.

Proof-freshness windows:

- Sanctions ≤ 24h.
- Residency credential ≤ 12 months.

Per-wallet caps & velocity: By risk tier and corridor.

Privacy availability: Mode 0 (public) is the global default.

- Mode 1 (amount-confidential) is opt-in globally unless a corridor/asset forbids it.

- Mode 2 (selective disclosure) is opt-in only where local law and venue policy permit.

Travel-Rule requirement: Corridor-specific (on/off; VASP-only vs. credentialed self-custody permitted).

Attestation options: TEEs are optional for public wallets; they may be required for institutional gateways in specific corridors.

9. GOVERNANCE

9.1 Objectives

Gurufin governance is designed for safety, legibility, accountability, and liveness.

The system separates parameter governance (frequent, low-risk changes) from protocol upgrades (infrequent, high-assurance changes) and provides transparent controls over treasury and program budgets.

9.2 Actors & roles

GXN holders: Ultimate authority; propose and vote. Voting power is delegable (liquid delegation) and revocable at any time.

Validators: Secure the network; may co-sign upgrade payloads and run emergency drills; no unilateral policy power.

Foundation: Stewards roadmaps and public goods; submits proposals with rationale and disclosures.

Security Council (n-of-m multisig): Narrowly scoped, time-bounded emergency powers[53].

Members include independent external signers; actions auto-expire unless ratified on-chain.

9.3 Proposal lifecycle (parameter changes & budgets)

Draft & review (off-chain): Forum/RFC with motivation, impact, diffs, and monitoring plan.

On-chain submission: Includes parameter JSON (or budget schedule), a proposal bond (anti-spam), and projected telemetry.

Voting window:

- Seven days
- Quorum
- Thresholds enforced (illustrative defaults below).

Timelock:

- 72 hours before execution.
- Monitoring alerts fire during the lock.

Execution: The Governance module applies changes atomically; the Parameter Registry records a signed, versioned diff.

Post-change report: Effect on metrics (fees, slippage, Oracle dispersion, utilisation) within a stated observation window.

Illustrative thresholds (governed):

- Quorum ≥ 10% of staked GXN voting power.
- Pass threshold >50% yes (excluding abstain).

Proposal bond is returned if the proposal reaches quorum; otherwise burned to discourage spam.

9.4 Parameter Registry (versioned)

All tunables live in a single, on-chain registry with typed schemas and machine-readable diffs:

Fee & PEG:

- $gfiat^{L1}$.
- $gfiat^{Asset}$.
- CPI cadence/cap.
- Fee bands.
- Gas rounding.

[53] §10.7

- Load multipliers.

Oracle: Provider sets:

- Quorum.
- τ_max (staleness).
- Deviation bands.
- Aggregation rule.
- Slashing tiers.

Market structure: CFMM amplification *A* by:

- Pair class.
- Arb trigger *s*trig.
- Parity band *δ*parity.
- Pool fee tiers.
- Inventory bands/caps.

Interop: Canonical channels per:

- Asset.
- Route risk weights.
- Gateway limits.

Privacy & compliance:

- Privacy availability (Mode 0/1/2).
- Corridor policies.
- Travel Rule toggles.

Relayers & paymasters: Per:

- Packet caps.
- Subsidy budgets.
- Rate limits.

Treasury/budgets: annual caps for:

- Ecosystem/Operations,
- bootstrap emission envelopes,
- grant templates.

Every change emits:

- *Parameter name.*
- *Old→new value.*
- *Proposer.*
- *Vote hash.*
- *Block height.*
- *Timelock*
- *Id.*
- *Human-readable rationale.*

9.5 Treasury & disbursements

Accounts & buckets: Foundation, Ecosystem, Network Operations, Oracle Reward, and Program Escrows are managed as distinct on-chain accounts.

Disbursement rules:

- Milestone-based streaming (vesters).
- Multisig approvals.
- Public invoices (hash-anchored).

Caps: Governance-set annual ceilings:

≤ X% of treasury per 12 months, per bucket

Transparency:

- Quarterly reports:
    - Spend.
    - Recipients.
    - KPI's.
- Plus, real-time dashboards for balances.
- Unlock calendars.
- Run-rates.

9.6 Protocol upgrades (consensus, VM, critical modules)

Stage 1: Spec & audit: Formal spec + public audits; test vectors published.

Stage 2: Testnet: Feature gates, load tests, and chaos drills; release candidate tagged.

Stage 3: Governance vote: Higher bar e.g.:

quorum 20%,

supermajority ≥66%

yes

Stage 4: Timelocked schedule:

- Coordinated activation window.
- Validator readiness attested.

Stage 5: Activation & rollback plan.

- Shadow telemetry;
- Pre-agreed rollback height retained for a short window.

Upgrades cannot seize user funds or alter balances; only code paths and parameters within declared scope may change.

9.7 Emergency controls (narrow, auditable, time-boxed)

Used for operational safety, not policy-making.

Examples:

- *Oracle degradation*: Freeze PEG drift, widen slippage guards, raise minimum gas, and throttle affected pairs.

- *Market integrity*: Pause a specific pool/corridor or non-canonical route on an extreme basis/Oracle disagreement.

- *Network health*: Rate-limit Mempool classes to absorb volumetric spam.

Constraints:

i. Actions are enumerated in the module (no arbitrary calls).

ii. Require Security Council n-of-m signatures with external members.

iii. Auto-expire (e.g., 72h) unless ratified by a token vote.

iv. Full event log:

a. Reason codes.
b. Scope.
c. Start/stop times.
d. Signers.
e. Post-mortem disclosure required.

9.8 Delegation & reputation

GXN holders can delegate voting power to representatives (single or split delegation).

Delegates expose public mandates and vote histories.

Delegators may override on a per-proposal basis.

A soft reputation layer (participation, alignment with outcomes) is published to the governance portal to help holders choose delegates.

9.9 Elections & registries

Oracle provider registry:

- Candidates post bonds.
- Voters confirm/rotate providers.
- Poor performers can be ejected via slashing + vote.

Relayer registry:

- Whitelists with caps and health SLAs;
- Rotation schedules are governed.

Canonical asset registry: Preferred routes per currency; listing/delisting by vote with explicit risk notes.

9.10 Governance, security & anti-spam

Economic spam guards: Proposal bonds, min content requirements, rate limiting.

Sybil resistance: Voting power derives from staked GXN; delegates publicly identified.

Upgrade safety: Staged rollouts with canary chains and determinism checks.

Conflict disclosures: Proposers disclose affiliations and economic interests; the portal flags conflicts.

9.11 Initial governance constants (illustrative; to be ratified)

Quorums, thresholds, timelocks, parameter changes (non-economic):

quorum 20% of bonded voting power

pass >50% YES

Timelock 72h

Economic/fee/emissions parameters:

quorum 30% of bonded voting power

pass >60% YES

Timelock 96h.

Chain upgrades / hard forks:

quorum 40% of bonded voting power

pass ≥66.7% YES

Timelock 120h

Global veto:

≥33.4%

NO-with-veto fails any proposal

Emergency actions:

auto-expiry 72h

ratification window 7 days

(persist on pass; otherwise auto-revert).

Using bonded voting power (not total supply) avoids quorum dilution from idle balances and aligns with DPoS security.

Proposal deposits (anti-spam; refunded at quorum): Set deposits dynamically so they remain meaningful across price cycles.

Refund 100% if quorum is met; partial slash for spam/abuse.

Base (most parameter proposals):

max(0.000002 × total_supply) - floor ≈ 200,000 GXN.

Economic / emissions / treasury proposals:

max(0.00001 × total_supply) - floor ≈ 1,000,000 GXN.

Chain upgrades / hard forks:

max(0.00003 × total_supply) - floor ≈ 3,000,000 GXN.

Co-sponsor guard (upgrades):

require ≥5 co-sponsors

holding ≥0.5% combined bonded power to submit.

Refund/slash policy:

100% refund at quorum

50% slash if flagged as spam (on-chain reason code)

or

duplicate failures inside 30 days.

Treasury caps & disclosure: Annual disbursement caps per treasury bucket (Foundation, Ecosystem, Node Pool, R&D) are published at the year start; mid-year review by governance.

Monthly on-chain report (openings, inflows, outflows, commitments, runway) plus independent audit at least annually.

All constants above are illustrative starting points; changes follow the governance process[54] *:*

proposal → vote → Timelock → execute

9.12 Disclosures & archives

All proposals, votes, diffs, audits, emergency events, and treasury movements are permanently archived, hash-linked, and available via public APIs.

A yearly Governance Review summarises significant changes, incidents, metrics, and lessons learned.

[54] *§10*

10. GURUFIN TOKENOMICS

Tokenomics is the economic framework by which a blockchain project aligns incentives across users, validators, governance, and other ecosystem participants.

10.1 Introduction

In the case of Gurufin, the native token GXN plays multiple critical roles: gas payment, staking asset, governance coin, and settlement currency, and is engineered to deliver predictable fees, sustainable rewards, and deflationary pressure.

This layered fee mechanism (Guru-PEG), and strong sinks via a verifiable burn address (GAL, the Gurufin Abyss Ledger).

10.2 Token Utility & Distribution

10.2.1 Roles of GXN

Gas Token: GXN is the base-layer token used to pay transaction fees, stabilized via Guru-PEG, to reduce fee volatility and offer predictable cost to end users.

Staking Asset: Validators stake GXN to secure consensus; delegators may delegate to validators and share rewards.

Governance Coin: GXN holders vote on protocol parameters, upgrades, and fee/gas configuration.

Settlement Currency: GXN is used in cross-chain transactions, protocol fees (including relayers/paymasters), and station activities.

10.2.2 Total Supply & Allocation

Maximum Supply (Genesis):

100,000,000,000 GXN.

No.	Category	Allocated Token	Ratio
1	Ecosystem Funds	27,000,000,000	27.00%
2	Network Operations	3,000,000,000	3.00%
3	Node Pool	25,000,000,000	25.00%
4	Team & Developers	19,500,000,000	19.50%
5	Advisors	2,000,000,000	2.00%
6	Gurufin Foundation	5,000,000,000	5.00%
7	Early Ecosystem Investment	3,000,000,000	3.00%
8	Strategic Investment	12,500,000,000	12.50%
9	Reserve	3,000,000,000	3.00%

Table 3 Token Allocation Breakdown

10.2.3 Supply & allocation (at TGE)

The initial allocation and locks/vesting below are inherited from the prior token schedule.

Percentages sum to 100% of the 100B max supply:

TGE: Token Generation

Event Vesting: Team & advisors, strategic partners, and ecosystem programs subject to multi-year vesting schedules with cliffs and linear release to ensure gradual unlocks and to mitigate early sell-pressure.

10.3 Staking & Unstaking

Gurufin uses a Delegated Proof of Stake (DPoS) consensus model. Validators must lock a minimum amount of GXN; delegators can delegate their stake to validators.

Rewards, Validators + delegators earn: Emission rewards from the Node Pool (25% allocation).

Fee Revenue from gas, cross-chain settlements, relayer/paymaster fees.

Validators earn:

(i) Staking rewards from the Node Pool.
(ii) Fee revenue[55].

Slashing for downtime/double-signing applies per protocol policy.

Slashing: Misbehaviour (double-signing, downtime) leads to *slashing* of validator stake & loss of partial rewards for delegators.

Unstaking: Delegators may withdraw (undelegate and reclaim) both principal and accrued rewards after epoch boundaries (or other governance-defined intervals).

10.4 Bridging

IBC-first approach: For trust-minimized, proof-based cross-chain settlement.

Gateway contracts: For non-IBC compatible chains / external assets; wrappers with canonical registry to ensure asset uniqueness and consistency.

Relayers & Paymasters: Per-packet incentives; paymasters may sponsor full multi-leg trades so that users pay in source asset with all-inclusive pricing.

Governance Oversight: Limits & caps for non-canonical or gateway routes; subsidy programs for strategic lanes and bootstrap of corridors.

10.5 Gas Pricing (Guru-PEG) & Gas In GXN

10.5.1 Formal Fee Formula

Define:

$g_{fiat}(tx)$= target fee in fiat

e.g.:

USD for transaction type tx.

$FX_{\frac{GXN}{USD^t}}$= Oracle−provided exchange rate of GXN to USD at time t

A. Base gas (Guru-PEG)

Gas paid in GXN is pegged in fiat by adjusting the GXN amount per tx.

Then:

$$\text{GasTarget}_{GXN^{(tx,t)}} = \frac{g_{fiat}(tx)}{FX_{\frac{GXN^{(t)}}{USD}}}$$

Fee floors and ceilings are maintained via guard rails, adjusting for consumer price index (CPI) to preserve real value over time. With CPI-indexed steps (cap) and change-rate guards[56]. This keeps:

L1 sends ≈ $0.013

and

$\frac{asset}{NFT}$ *ops ≈ $0.040*

** Illustrative defaults*

B. Station/DEX fees

Swap fees are tiered by pair class, e.g.:

2–5 bps for stable↔stable.

slightly higher for stable↔GXN/long-tail.

[55] §9.5

[56] §4

RFQ routes may quote bespoke spreads for size. Fees accrue in the transacted asset and are shared to LPs and the protocol per pool policy.

C. Relayer and paymaster

Cross-chain PvP settlement pays modest per-packet relayer fees; a paymaster can bundle and net multi-leg Costs are so high that users pay "all-in" for the source asset[57].

Governance can subsidise specific corridors from Ecosystem/Operations buckets are strategic.

D. Sinks & treasury

Collected GXN fees are used for:

i. Validator/infra operations.
ii. Protocol/oracle upkeep.
iii. Burn to.

10.5.2 Service Classes & Buckets

Transactions are grouped by service class, e.g:

- L1 transfer.
- Asset/NFT operation.
- swap (DEX).
- Cross-chain settlement.
- Station activity.

Each class has a preset g_{fiat} target, e.g:

$0.013 for basic transfers.

$0.040 for asset ops.

For higher complexity operations, additional "complexity multipliers" may apply (computation, bandwidth, storage usage).

10.5.3 Storage & Rebate Mechanics

Users pay for storage (on chain or state channels).

Rebate mechanism: When data states are closed, channels pruned, or storage freed, a portion of storage charge is refunded to the user.

Storage charges & rebate percentages are governed, with a small non-refundable fraction to cover overhead.

10.5.4 Minimum Fee Floors & Congestion Multipliers

A minimum fee per transaction class in GXN (via the above formula) ensures anti-spam and cost coverage.

Under congestion, dynamic multipliers may apply, e.g:

$$\times 1.5,$$

or

$$\times 2$$

Depending on utilisation thresholds, e.g:

$$> 80\ \%\ utilization$$

To prioritize transactions and protect the quality of service.

10.6 Fee Structure, Sinks, and Economic Sustainability

10.6.1 Fee Structure

DEX / Swap Fees e.g.:

2-5 basis points (bps) for stable-to-stable pairs.

higher for stable ↔ GXN or long-tail asset pairs.

Cross-Chain / Relayer / Paymaster Fees: Per-packet fees; paymasters optimize cost for users, possibly absorbing part of the fees in competitive corridors.

10.6.2 Burn Sink (GAL)

A portion of all collected GXN fees is burned permanently to the Gurufin Abyss Ledger (GAL), a keyless on-chain burn address.

Application: From transaction fees, station fees, and cross-chain fees. The proportion of fee revenue destined for burn is defined via governance parameters.

10.6.3 Economic Alignment and Stakeholder Incentives

Users gain predictable fiat-like fees, with near-zero gas for stablecoin transfers, and optimal routing.

Validators earn initial emissions (25%) plus an increasing share of fee revenue as usage grows.

Liquidity providers (LPs) receive swap fees; strategic emissions may top-up rewards during early liquidity bootstrapping.

[57] *§4.6*

Builders, Partners, and Ecosystem are incentivized via the 20% Ecosystem Development allocation.

Long-term holders benefit from burn mechanisms (deflationary pressure) and value accrual from a growing fee base.

10.7 Governance & Transparency

All core parameters (fee targets g_{fiat}, FX oracle policy, burn percentages, congestion thresholds, validator commission rates, emission schedules) are subject to on-chain governance with *timelocks*.

Public dashboards will provide machine-readable data:

- Unlock & vesting schedules.
- Emission vs consumption.
- Burn totals, circulating vs total supply.
- Treasury balances.

Auditability and external verification are encouraged for oracles and gateway contracts.

10.8 Related Academic Foundations & Design Justifications

Many recent studies emphasize the importance of multidimensional fee markets, e.g:

- Pricing computation.
- Storage.
- Bandwidth separately, to better align fees with resource costs.

Empirical work shows that when block or resource utilization exceeds high thresholds (e.g. 90 %), fees rise non-linearly. This supports our use of congestion multipliers & minimum floors to maintain service levels.
Research into fee stability and predictability indicates that tying fees to fiat or predictable reference points helps reduce volatility risk for end users.

10.9 Incentive programs

• *LP incentives (fee-first, emissions-as-needed):* Liquidity providers earn pool swap fees as the primary, sustainable reward (fee tiers by pair class[58]).

Governance may deploy time-bounded GXN top-ups from the Ecosystem bucket to bootstrap depth in strategic corridors. Inventory bands and per-LP caps mitigate concentration; bonded LP positions can receive boosts.

• *Builders & public goods:* Ecosystem allocation funds SDKs, wallets, indexers, relayers, market-quality keepers, and audits.

Grants are milestone-based, streamed, and disclosed via the treasury dashboard.

• *Oracle providers (bonded reporters):* Reporters post a GXN bond and earn per-submission rewards from an Oracle Reward budget funded by:

(i) A small protocol skim of Station fees and/or.
(ii) A governed Network Operations/Ecosystem line item. Payouts are quality-weighted (timeliness/dispersion), with slashing for staleness, outliers, or equivocation[59].

• *Relayers & paymasters:* IBC relayers receive per-packet fees; governance may run targeted subsidy pools for retail corridors during ramp-up.

Paymasters may earn a small spread or service fee for quoting "all-in" UX, subject to caps and disclosure.

• *Segregation of funds:* The Node Pool (staking) remains dedicated to validator security/emissions and is not a routine source of LP or oracle incentives. All incentive budgets, caps, and run-rates are parameterised and disclosed on-chain.

Summary

The Gurufin Tokenomics model seeks to blend:

i. Predictability (via Guru-PEG, fixed fees for compliance chains)
ii. Sustainability (staking rewards + growing fee revenue)
iii. Deflationary pressure (via GAL burns)
iv. Incentive alignment across all stakeholders
v. Combined, these features aim to ensure Gurufin's long-term network security, adoption, and utility in financial market infrastructure (FMI) and beyond.

[58] *§6*

[59] §5

11. REFERENCES

[1] R. Cheng *et al.*, "Ekiden: A Platform for Confidentiality-Preserving, Trustworthy, and Performant Smart Contract Execution," *Proceedings - 4th IEEE European Symposium on Security and Privacy, EURO S and P 2019*, pp. 185–200, Aug. 2019, doi: 10.1109/EuroSP.2019.00023.

[2] "IBC - Ecosystem - Cosmos: The Internet of Blockchains." Accessed: Sep. 03, 2025. [Online]. Available: https://cosmos.network/ibc/

[3] C. Goes, "The Interblockchain Communication Protocol: An Overview," Jun. 2020, Accessed: Sep. 03, 2025. [Online]. Available: https://arxiv.org/pdf/2006.15918

[4] Y. Zeighami *et al.*, "Impact of Weight Loss on Brain Age: Improved Brain Health Following Bariatric Surgery," *Neuroimage*, vol. 259, Dec. 2021, doi: 10.1016/j.neuroimage.2022.119415.

[5] C. Yin *et al.*, "Atomic Smart Contract Interoperability with High Efficiency via Cross-Chain Integrated Execution," *IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS*, vol. XX, p. 1, Feb. 2025, Accessed: Sep. 03, 2025. [Online]. Available: https://arxiv.org/pdf/2502.12820

[6] R. Cheng *et al.*, "Ekiden: A Platform for Confidentiality-Preserving, Trustworthy, and Performant Smart Contract Execution," *Proceedings - 4th IEEE European Symposium on Security and Privacy, EURO S and P 2019*, pp. 185–200, Aug. 2019, doi: 10.1109/EuroSP.2019.00023.

[7] S. Goldwasser, S. Micali, and C. Rackoff, "Knowledge complexity of interactive proof systems," *SIAM Journal on Computing*, vol. 18, no. 1, pp. 186–208, Jul. 1989, doi: 10.1137/0218012;WGROUP:STRING:PUBLICATION.

[8] V. Costan and S. Devadas, "Intel SGX Explained," *Cryptology ePrint Archive*, 2016, Accessed: Sep. 03, 2025. [Online]. Available: https://eprint.iacr.org/2016/086

[9] H. Adams, N. Zinsmeister, and D. Robinson, "Uniswap v2 Core," 2020.

[10] V. A. Vassiliev, "Complements of discriminants of real parabolic function singularities," Aug. 2022, Accessed: Sep. 03, 2025. [Online]. Available: https://arxiv.org/pdf/2208.10929

[11] "BANK FOR INTERNATIONAL SETTLEMENTS DELIVERY VERSUS PAYMENT IN SECURITIES SETTLEMENT SYSTEMS," 1992.

[12] "BANK FOR INTERNATIONAL SETTLEMENTS SETTLEMENT RISK IN FOREIGN EXCHANGE TRANSACTIONS Report prepared by the Committee on Payment and Settlement Systems of the central banks of the Group of Ten countries Basle," 1996.

[13] B. Biais, L. Glosten, and C. Spatt, "Market microstructure: A survey of microfoundations, empirical results, and policy implications," *Journal of Financial Markets*, vol. 8, no. 2, pp. 217–264, May 2005, doi: 10.1016/J.FINMAR.2004.11.001.

[14] L. R. Glosten and P. R. Milgrom, "Bid, ask and transaction prices in a specialist market with heterogeneously informed traders," *J financ econ*, vol. 14, no. 1, pp. 71–100, Mar. 1985, doi: 10.1016/0304-405X(85)90044-3.

[15] S. A. Ross, "The arbitrage theory of capital asset pricing," *J Econ Theory*, vol. 13, no. 3, pp. 341–360, Dec. 1976, doi: 10.1016/0022-0531(76)90046-6.

[16] C. Xu, Z. Chen, J. Mai, X. Xu, and S. He, "Pose- and Attribute-consistent Person Image Synthesis," *ACM Transactions on Multimedia Computing, Communications and Applications*, vol. 19, no. 2s, Feb. 2023, doi: 10.1145/3554739.

[17] C. Xu, Z. Chen, J. Mai, X. Xu, and S. He, "Pose- and Attribute-consistent Person Image Synthesis," *ACM Transactions on Multimedia Computing, Communications and Applications*, vol. 19, no. 2s, Feb. 2023, doi: 10.1145/3554739/ASSET/400A4A81-F36C-4704-AF97-E46778E581DB/ASSETS/IMAGES/LARGE/TOMM-2021-0454-F13.JPG.

[18] M. Yaghoobi and M. Alaei, "Machine learning for compositional disorder: A comparison between different descriptors and machine learning frameworks," *Comput Mater Sci*, vol. 207, May 2022, doi: 10.1016/j.commatsci.2022.111284.

[19] "ibc/spec/app/ics-020-fungible-token-transfer at main · cosmos/ibc · GitHub." Accessed: Sep. 03, 2025. [Online]. Available: https://github.com/cosmos/ibc/tree/main/spec/app/ics-020-fungible-token-transfer?utm_source=chatgpt.com

[20] "ibc/spec/app/ics-020-fungible-token-transfer at main · cosmos/ibc · GitHub." Accessed: Sep. 04, 2025. [Online]. Available: https://github.com/cosmos/ibc/tree/main/spec/app/ics-020-fungible-token-transfer?utm_source=chatgpt.com

[21] C. Xu, Z. Chen, J. Mai, X. Xu, and S. He, "Pose- and Attribute-consistent Person Image Synthesis," *ACM Transactions on Multimedia Computing, Communications and Applications*, vol. 19, no. 2s, Feb. 2023, doi: 10.1145/3554739.

[22] A. Madhavan, "Market microstructure: A survey," *Journal of Financial Markets*, vol. 3, no. 3, pp. 205–258, Aug. 2000, doi: 10.1016/S1386-4181(00)00007-0.

[23] F. Schär, "Decentralized finance: on blockchain-and smart contract-based financial markets," *Federal Reserve Bank of St. Louis Review*, vol. 103, no. 2, pp. 153–174, 2021, doi: 10.20955/R.103.153-74.

[24] H. Adams, N. Zinsmeister, M. Salem moody, uniswaporg River Keefer, and D. Robinson, "Uniswap v3 Core," 2021.

[25] S. Eskandari, M. Salehi, W. C. Gu, and J. Clark, "SoK: Oracles from the Ground Truth to Market Manipulation," *AFT 2021 - Proceedings of the 2021 3rd ACM Conference on Advances in Financial Technologies*, pp. 127–141, Sep. 2021, doi: 10.1145/3479722.3480994.

[26] H. Adams, N. Zinsmeister, M. Salem moody, uniswaporg River Keefer, and D. Robinson, "Uniswap v3 Core," 2021.

[27] D. Bai, J. Cao, Y. Cao, L. Wen, and M. Stojmenovic, "Ormer: A Manipulation-resistant and Gas-efficient Blockchain Pricing Oracle for DeFi," Oct. 2024, Accessed: Sep. 04, 2025. [Online]. Available: https://arxiv.org/pdf/2410.07893

[28] B. Biais, L. Glosten, and C. Spatt, "Market microstructure: A survey of microfoundations, empirical results, and policy implications," *Journal of Financial Markets*, vol. 8, no. 2, pp. 217–264, May 2005, doi: 10.1016/J.FINMAR.2004.11.001.

[29] R. Song and B. CC, "LinkDID: A Privacy-Preserving, Sybil-Resistant and Key-Recoverable Decentralized Identity Scheme," Jul. 2023, Accessed: Sep. 08, 2025. [Online]. Available: https://arxiv.org/pdf/2307.14679

[30] S. Fischer, D. Megías, G. Wang, and G. Zhang, "An Efficient Distributed Identity Selective Disclosure Algorithm," *Applied Sciences 2025, Vol. 15, Page 8834*, vol. 15, no. 16, p. 8834, Aug. 2025, doi: 10.3390/APP15168834.

[31] J. Ménétrey *et al.*, "Attestation Mechanisms for Trusted Execution Environments Demystified," *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, vol. 13272 LNCS, pp. 95–113, Sep. 2022, doi: 10.1007/978-3-031-16092-9_7.

[32] Y. Xiao, N. Zhang, J. Li, W. Lou, and Y. T. Hou, "PrivacyGuard: Enforcing Private Data Usage Control with Blockchain and Attested Off-chain Contract Execution," *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, vol. 12309 LNCS, pp. 610–629, Apr. 2019, doi: 10.1007/978-3-030-59013-0_30.

[33] C. Lee *et al.*, "Design of Blockchain-based Travel Rule Compliance System," Apr. 2022, Accessed: Sep. 08, 2025. [Online]. Available: https://arxiv.org/pdf/2204.13508

[34] "The Travel Rule and KYB in Crypto: A Complete Compliance Guide." Accessed: Sep. 08, 2025. [Online]. Available: https://www.dotfile.com/blog-articles/the-travel-rule-and-kyb-in-crypto-a-complete-compliance-guide?utm_source=chatgpt.com

[35] "Keeping crypto clean: risk-based controls for stablecoins | Reuters." Accessed: Sep. 08, 2025. [Online]. Available: https://www.reuters.com/legal/legalindustry/keeping-crypto-clean-risk-based-controls-stablecoins-2025-06-24/?utm_source=chatgpt.com

[36] "KYC and AML Compliance for Fintechs: 2024 Guide — Castellum.AI." Accessed: Sep. 08, 2025. [Online]. Available: https://www.castellum.ai/insights/kyc-aml-fundamentals-for-fintechs-2024?utm_source=chatgpt.com

[37] E. Ong and J. Kubiatowicz, "Optimizing Robustness While Generating Shared Secret Safe Primes," *Lecture Notes in Computer Science*, vol. 3386, pp. 120–137, 2005, doi: 10.1007/978-3-540-30580-4_9.

[38] J. S. Warford, D. Vega, and S. M. Staley, "A Calculational Deductive System for Linear Temporal Logic," *ACM Comput Surv*, vol. 53, no. 3, May 2021, doi: 10.1145/3387109/SUPPL_FILE/WARFORD.ZIP.

[39] P. A. Grassi *et al.*, "Withdrawn NIST Technical Series Publication Warning Notice Withdrawn Publication Series/Number NIST Special Publication 800-63B Title Digital Identity Guidelines: Authentication and Lifecycle Management Publication Date(s) Superseding Publication(s) (if applicable)," 2017, doi: 10.6028/NIST.SP.800-63B-4.

[40] "Cosmos: The Internet of Blockchains." Accessed: Sep. 08, 2025. [Online]. Available: https://cosmos.network/whitepaper/

[41] V. Buterin and V. Griffith, "Casper the Friendly Finality Gadget," Oct. 2017, Accessed: Sep. 08, 2025. [Online]. Available: https://arxiv.org/pdf/1710.09437

[42] P. Brendler, "Rising earnings inequality and optimal income tax and social security policies," *J Monet Econ*, vol. 134, pp. 35–52, Mar. 2023, doi: 10.1016/J.JMONECO.2022.10.004.

[43] "ETHEREUM: A SECURE DECENTRALISED GENERALISED TRANSACTION LEDGER".

[44] "Hub & Spoke Liquidity: In search of the perfect cross-chain model | by Squid | Medium." Accessed: Sep. 08, 2025. [Online]. Available: https://medium.com/%40squidrouter/hub-spoke-liquidity-in-search-of-the-perfect-cross-chain-model-d648037eb5cf

[45] "How Axelar Keeps you Safe During Emergencies | Axelar Blog." Accessed: Sep. 08, 2025. [Online]. Available: https://www.axelar.network/blog/hub-and-spoke-architecture?utm_source=chatgpt.com

[46] "Solving Gas Fee Volatility with Stablecoins - HeLa." Accessed: Sep. 08, 2025. [Online]. Available: https://helalabs.com/blog/solving-gas-fee-volatility-with-stablecoins/?utm_source=chatgpt.com

[47] D. Crapis, C. C. Moallemi, and S. Wang, "Optimal Dynamic Fees for Blockchain Resources," Sep. 2023, Accessed: Sep. 08, 2025. [Online]. Available: https://arxiv.org/pdf/2309.12735

[48] M. V. X. Ferreira, D. J. Moroz, D. C. Parkes, and M. Stern, "Dynamic Posted-Price Mechanisms for the Blockchain Transaction Fee Market," *AFT 2021 - Proceedings of the 2021 3rd ACM Conference on Advances in Financial Technologies*, pp. 86–99, Nov. 2021, doi: 10.1145/3479722.3480991.

[49] A. Laurent, L. Brotcorne, and B. Fortz, "Transaction fees optimization in the Ethereum blockchain," *Blockchain: Research and Applications*, vol. 3, no. 3, p. 100074, Sep. 2022, doi: 10.1016/J.BCRA.2022.100074.

[50] H. Fan *et al.*, "QoS-pro: A QoS-enhanced Transaction Processing Framework for Shared SSDs," *ACM Transactions on Architecture and Code Optimization*, vol. 21, no. 1, Jan. 2024, doi: 10.1145/3632955/ASSET/206B3809-BFE4-4360-A424-7546FD854894/ASSETS/IMAGES/LARGE/TACO-2023-39-F18.JPG.

[51] "ibc/spec/relayer/ics-018-relayer-algorithms/README.md at main · cosmos/ibc · GitHub." Accessed: Sep. 08, 2025. [Online]. Available: https://github.com/cosmos/ibc/blob/main/spec/relayer/ics-018-relayer-algorithms/README.md?utm_source=chatgpt.com

[52] "The Blockchain Oracle Problem | Chainlink." Accessed: Sep. 08, 2025. [Online]. Available: https://chain.link/education-hub/oracle-problem?utm_source=chatgpt.com

[53] C. Douligeris and A. Mitrokotsa, "DDoS attacks and defense mechanisms: classification and state-of-the-art," *Computer Networks*, vol. 44, no. 5, pp. 643–666, Apr. 2004, doi: 10.1016/J.COMNET.2003.10.003.

[54] R. F. Almgren, "Optimal execution with nonlinear impact functions and trading-enhanced risk," *Appl Math Finance*, vol. 10, no. 1, pp. 1–18, Mar. 2003, doi: 10.1080/135048602100056;WEBSITE:WEBSITE:TFOPB;PAGEGROUP:STRING:PUBLICATION.

[55] "Stable Pool | Balancer." Accessed: Sep. 09, 2025. [Online]. Available: https://docs.balancer.fi/concepts/explore-available-balancer-pools/stable-pool/stable-pool.html?utm_source=chatgpt.com

[56] "Hub-spoke network topology in Azure - Azure Architecture Center | Microsoft Learn." Accessed: Sep. 09, 2025. [Online]. Available: https://learn.microsoft.com/en-us/azure/architecture/networking/architecture/hub-spoke?utm_source=chatgpt.com

[57] M. Egorov, "StableSwap-efficient mechanism for Stablecoin liquidity," 2019.

[58] "Exploring Autonomous System Numbers-The Internet Protocol Journal - Volume 9, Number 1 - Cisco Systems." Accessed: Sep. 09, 2025. [Online]. Available: https://www.potaroo.net/papers/ipj/2006-v9-n1-asns/asns.html

[59] E. Buchman, J. Kwon, and Z. M. Tendermint, "The latest gossip on BFT consensus," Jul. 2018, Accessed: Sep. 09, 2025. [Online]. Available: https://arxiv.org/pdf/1807.04938

[60] "Why Do VASPs Need InterVASP Messaging Standard (IVMS 101)? — OpenVASP Association." Accessed: Sep. 09, 2025. [Online]. Available: https://www.openvasp.org/blog/why-do-vasps-need-intervasp-messaging-standard-ivms-101

[61] "interVASP Messaging." Accessed: Sep. 09, 2025. [Online]. Available: https://www.intervasp.org/

Appendix: Glossary

(rhoP) p*	System Use (demand/Capacity)	MEV	Maximal Extraction Value
ABCI	Application Blockchain Interface	MPC	Multi-Party Computation
AMM	Automated Market Makers	NCOF	Net Cash Out Flow
ASF	Available Stable Funding	NFT	Non-Fungible Token
APY	Annual Percentage Yield	NSFR	Net Stable Funding Ratio
BFT	Byzantine Fault Tolerance	Oracle	Supplies blockchains with off-chain data
BIS	Bank of International Settlements	Opt-in	Voluntary mechanism with explicit user consent
Bridge Risk	Risk assets face when crossing two systems	Paymaster	Smart contract that pays the gas fees
Cannonical	Official or accepted version of data	PEG	Price Equilibrium Governance
CCTP	Cross-Chain Transfer Protocol.	PEP	Politically Exposed Person
CEX	Centralized Exchange	PII	Personal Identifiable Information
CFMM	Constant Function Market Maker	Playbook	Set of standardised actions and responsibilities
Compress Spreads	Increasing liquidity and reducing costs	PoAc	Proof of Activity
dApss	Decentralised Applications.	PoC	Proof of Compliance
Denom	Identifier or unit of account of a token or asset	PoET	Proof of Elapsed Time
DEX	Decentralized Exchange	PoS	Proof of Stake
DexAggregator	Protocol that sources liquidity across DEXs	PoW	Proof of Work
DID	Digital ID	PSP	Payment Service Providers
DoS	Denial of Service	PvP	Payment Vs Payment
DDoS	Distributed Denial of Service	q	Fiat
DPoS	Delegated Proof of Stake	REPO	Loan, which is sold and later repurchased
ES	Expected Shortfalls	RFQ	Request for Quotation
ETH	Ethereum	RPC	Remote Procedure Call
GatewayGX	Codename for a Token module	RSF	Required Stable Funding
EVM	Ethereum Virtual Machine	RTGS	Real Time Gross Settlement
FAFT	Financial Action Task Force	RWA	Real World Assets
FBA	Frequent Batch Authentication	S	Securities
FMI	Financial Market Infrastructure	SLA	Service Level Agreement
FSB	Financial Stability Board	SLOs	Service Level Objectives
h	Haircuts	T-Bills	Hours-52 weeks
Haircuts	Percentage applied to an asset market value	T-Bonds	20-30 Y
h_O	Cash Head Room	T-Notes	2-10Y
HQLA	High Quality Liquid Assets	TEE	Trusted Execution Environments
HSM	Hardware Secure Module	TGE	Token Generation Eent
IBC	Internet Blockchain Communication	TPS	Transactions Per Second.
Iddle Capital	Financial resources that are not earning returns	TTL	Time To Live
IP/ASN	Internet Protocol/Autonomous Service Number	TVL	Total Value Locked
ISP	Internet Service Provider	TWAMM	Time Weighted Market Maker
IVMS	Internet Vast Message Standard	TWAP	Time Weighted Average Price
KYC	Know Your Customer	VASP	Virtual Asset Service Provider
LCR	Liquid Cover Ratio	VWAPS	Volume-Weighted Average Price
Liquidity Fragm.	When liquidity is split across multiple venues	W3C	World Wide Web Consortium
LP	Liquidity Provider	zkProof	Zero-Knowledge Proof
LRS	Live Reserve Scanner	λ	Redemptions/day
M(t)	Maturity	μ	Service Rate
MemPool	Queue of pending transactions in the blockchain		

Appendix: Legal Notices & Risks (public summary)

The Gurufin protocol, the Gurufin defi hub and the GXN tokens described herein remain under development and may be subject to change. The features, tools, uses, functionality, and the mechanisms of distribution remain subject to review and further development. Access to some features may not be available in all jurisdictions.

Further, the GXN tokens described herein are not expected to have any rights, uses, purpose, attributes, functionalities, or features except for those which are specifically described in this whitepaper. GXN tokens are not investments and should not be viewed or treated as an investment, nor should they be purchased as a speculative investment. GXN is not designed to provide holders with distributions and does not represent a right to the assets, income or profits of any person. GXN tokens are intended for use in the Gurufin ecosystem by network participants and ecosystem collaborators for the purposes described herein.

THIS IS NOT AN OFFER TO SELL OR THE SOLICITATION OF AN OFFER TO PURCHASE ANY GXN TOKENS, AND IS NOT AN OFFERING, ADVERTISEMENT, SOLICITATION, CONFIRMATION, STATEMENT OR ANY FINANCIAL PROMOTION THAT CAN BE CONSTRUED AS AN INVITATION OR INDUCEMENT TO ENGAGE IN ANY INVESTMENT ACTIVITY. YOU SHOULD NOT RELY ON THE CONTENT HEREIN FOR ADVICE OF ANY KIND, INCLUDING LEGAL, INVESTMENT, FINANCIAL, TAX OR OTHER PROFESSIONAL ADVICE, AND SUCH CONTENT IS NOT A SUBSTITUTE FOR ADVICE FROM A QUALIFIED PROFESSIONAL.

THIS DOCUMENT CONTAINS HYPOTHETICAL, FORWARD-LOOKING AND/OR PROJECTED STATEMENTS AND/OR FIGURES WHICH ARE NOT GUARANTEED AND ARE SUBJECT TO CHANGE; THE ACTUAL PERFORMANCE OF THE GURUFIN ECOSYSTEM MAY VARY. GURUFIN MAKES NO REPRESENTATION OR WARRANTY, EXPRESS OR IMPLIED, AS TO THE COMPLETENESS, RELIABILITY, VALIDITY, OR ACCURACY OF THIS INFORMATION. ANY INFORMATION CONTAINED HEREIN IS SUBJECT TO CHANGE WITHOUT NOTICE.

CONTACT US

info@gurufin.com
contact@gurufin.com